CISO Series

Deception Technology – The Newest Addition to Your Cyber Defense Suite

Authored By: TrapX Security Operations Center

Date of Publication: March 30, 2015

TABLE OF CONTENTS

THE DEMOCRATIZATION OF CYBER SECURITY THREATS

The media has been replete with stories, almost on a weekly basis, of new data breaches across enterprise and government. New zero day events are discovered with regularity and the propagation of these attacks is fueled by easy access to advanced malware. These threats and others have changed our perceptions of the relative safety afforded by our current information security strategies. Most CISO's will admit that the perimeter cannot be defended with confidence anymore. We are now in the process of understanding not if we have been breached, but where and how.

This makes the CISO job all the more difficult. The CISO must stay ahead of organized crime, rogue nation states and the growing army of hacktivists and "script kiddies." Compliance remains a major administrative responsibility. The growing army of mobile users create more opportunities for advanced malware and APTs to penetrate the organization and put sensitive and confidential corporate data at serious risk.

"Overall, the larger trend that emerged in 2013 was that of the democratization of security threats, driven by the easy availability of malicious software and infrastructure that can be used to launch advanced targeted attacks. This ubiquity of security threats has led organizations to realize that traditional security approaches have gaps, thereby leading them to rethink and invest more in security technology."[1]

Ruggero Contu, Research Director, Gartner Group

[1] Gartner Group Press Release, August 22, 2014. "Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware"

Legacy Cyber Security Suites are Not Enough

Our legacy information security tools are failing to keep advanced persistent threats and advanced malware out of our core information networks and infrastructure. Traditional security architectures have not proven to be agile enough to meet these threats. Defense-in-depth cyber security software suites continue to grow, but they are proven less and less effective against the new breed of malware and advanced persistent threats attacking our core systems.

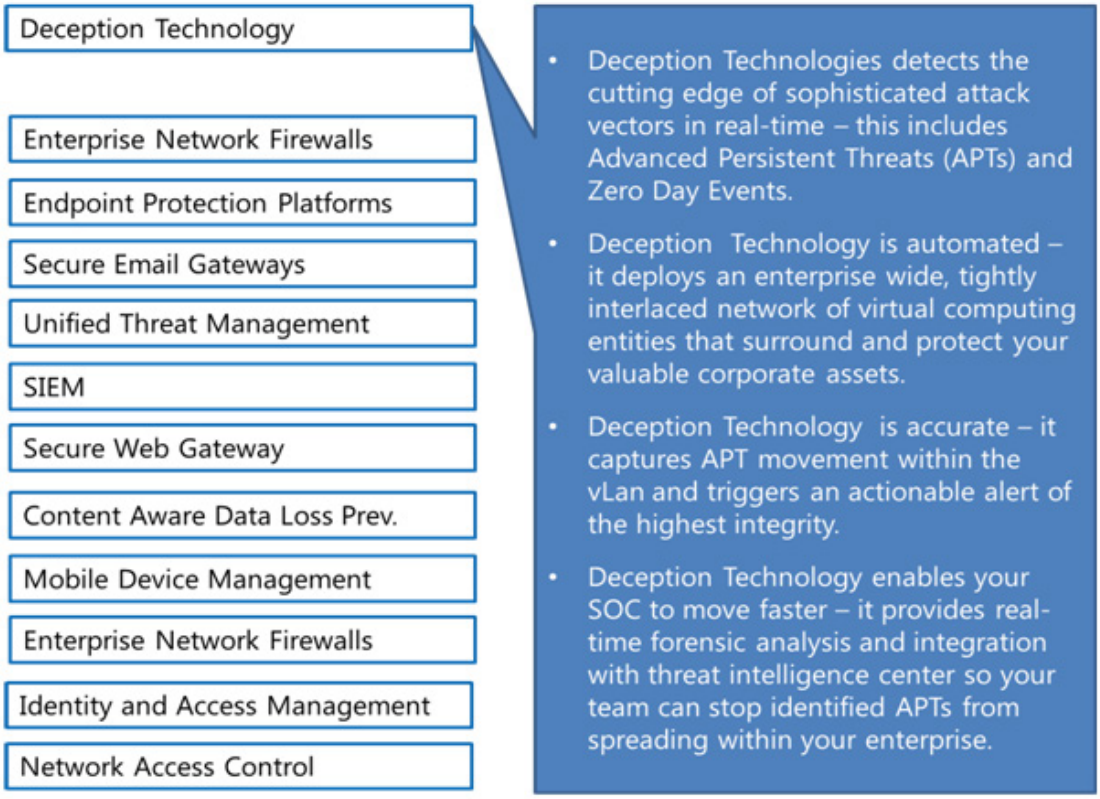
Under Fire in the Security Operations Center

All of this makes it increasingly difficult for your SOC team to protect your enterprise. The SOC team is swimming in alerts. Critical and important alerts, if your software can generate them, are often lost in a sea of alerts for compliance and malware that overwhelm most security operations centers. Security operations teams are becoming overwhelmed with an excess of big data. Many security operations centers note that they process hundreds, thousands or even millions of alerts per day. The volume of alerts has become so high that filtering out the noise is very difficult.

SOCs still do not have new tools that enable them to discover APTs or zero day events before the serious damage is done. APTs move silently through the organization and exfiltrate targeted data. APTs only need one entry point to get past the perimeter defense. Once inside, most of your legacy technology will absolutely not detect their movement in areas such as theVLAN. This is the center of the problem. APTs have the ability to move silently within the corporate network and can remain undetected for months or even years.

THE CURRENT INFORMATION SECURITY TAXONOMY

The current information security market has many categories of services and software. In 2014 worldwide information security spending reached almost $71.1 billion per Gartner Group. This includes worldwide security software revenue which in 2013 totaled $19.9 billion. Many of these existing services and technologies are integrated into your operations today. A new category, Deception Technology has emerged with the launch of new products such as TrapX Security's Deception Grid™. Deception Technology allows your SOC team to detect the most sophisticated attack vectors to include advanced persistent threats (APTs) and zero day events in real-time.



NEW BEST PRACTICES FOR YOUR SECURITY OPERATIONS CENTER

Current perimeter security has proven to be very vulnerable to some of today's APTs. To keep pace with these rapidly evolving attacks, deception technology has emerged as a new category of cyber defense that can uniquely empower security operations centers (SOCs) and response teams to deal with the APT challenge.

The earliest deception technology building blocks were based upon "honeypots." The notion of a honeypot came as a virtual infrastructure element designed solely for the purpose of attracting and identifying cyber intruders. These were point solutions, placed one at a time throughout the enterprise. If you wanted to emulate a Sybase® server you had to acquire a license for one. In fact you generally needed an operating system license or license for every instance you needed to blend into your existing network. The lack of automation, proprietary emulation and the large investment required for manual deployment made these too expensive to deploy at enterprise scale. The maintenance and configuration requirements were extreme; to even consider this level of effort at an enterprise scale was impractical. Yet, when the honeypot was touched by malware, the alert was extremely high confidence. It was clear that almost all of the time any positive alert was a clear indicator of a high risk event. At very limited scale and coverage, honeypots worked well to decisively identify bad actors within the enterprise.

"DeceptionGrid is the first real production of Honeypot 2.0 to reach the market. We fully automate deployment. All of the emulation set-up is all done for you. Our dashboard enables our enterprise customer to monitor multiple global domains or facilitate multi-customer management by MSSPs. Finally, our static and dynamic analysis and reporting are also fully automated. Everything you need is there now with much lower cost of ownership and operation."

Yuval Malachi

Founder & CTO, TrapX Security

[2] Gartner Group Press Release, June 10, 2014. "Gartner Says Worldwide Security Software Market Grew 4.9 Percent in 2013"

Honeypots did not lend themselves to speed of remediation either. Generally, they were standalone entities and did not have the capability to provide the forensic analysis. All of the data from an alert required a substantial amount of manual analysis to identify exactly the nature of the APT involved. The Tier 1 SOC had to escalate the data and bring in personnel that could do the forensic analysis. Time works against you in neutralizing an APT event – every day counts and it while early honeypot deployments produced positive benefits there was still significant room for improvement.

ADVANCED PERSISTENT THREATS (APTs)

An advanced persistent threat is a set of ongoing and clandestine computer hacking processes which are actively supported by a team of people and usually targeted to a specific entity. The term advanced persistent threat (or APT) actually originated within the United States Air Force in 2006 after being used first by Colonel Greg Rattray. The Department of Defense and Intelligence community normally need to assign classified names to specific threat actors. In order to communicate better with the uncleared personnel and the public the Air Force developed the term to refer to the general category of activity and associated malware.

APTs include a high level of sophistication and special malware that can exploit the smallest of vulnerabilities in the systems under attack. The goal of these APT attacks, of course, is to place malware (spyware) on one or more computer elements for an extended period of time, to utilize these elements to actively seek out valuable information for compromise, and then to extract (exfiltrate) that information. This information may set the stage for future damage to infrastructure or additional attacks.

"Clearly as advanced persistent threats have grown more sophisticated and capable the net result is that the concept of defending a perimeter seems to be failing at an increasing rate."

Carl Wright
EVP and General Manager, TrapX

Persistent means they almost always have a specific target in mind and they are continuously working to move their objectives forward. The APT generally includes a command and control component that is monitoring the process, communicating back to originating team ("bad actors") and ultimately extracting data from the specific target. This is not really an opportunistic attack – this is an attack targeted from the very beginning.

APT's always need an entry point for infection and establishment of a first anchor point. The first step is to establish a beachhead behind firewalls and with access to organizational files, databases and administration. Many channels provide opportunities for entry and infection especially with the increase in mobile technology. These channels include:

- Socially engineered attacks on employees;
- Additional risk in airports, hotels, coffee shops;
- Spearfishing with USB devices;
- Sophisticated attacks using encrypted malware and tunneling which is not identified by perimeter and filtering systems;
- Exploiting security holes in VPN devices bypassing perimeter security;
- Visibility to corporate devices such as open printers on wireless networks;
- Exploitation through 3rd party services; and,
- Phishing – all it takes is one click on a link by one employee to bring an APT into the organization.

Once inside the network then attackers can begin their task of reconnaissance. They begin to spread, identify key information, allow remote command and control, and ultimately support exfiltration of key data. Current perimeter security has proven to be very vulnerable to some of today's APTs. To keep pace with these rapidly evolving attacks, deception technology has emerged as a new category of cyber defense that can uniquely empower security operations centers (SOCs) and response teams to deal with the APT challenge.

UNDERSTANDING THE INTRUSION KILL CHAIN

The malicious tools the hackers use are constantly changing, yet the underlying methods used by sophisticated attackers are so predictable that the security research community has given this multistage chain of events its own name: the Intrusion Kill Chain. Technology blind spots have prevented most organizations from detecting, analyzing and disrupting the early and middle stages of the cyber kill chain.

The Intrusion Kill Chain has six steps that include:

Research – This is about target selection and determining the vectors that will be used to successfully infiltrate the target.

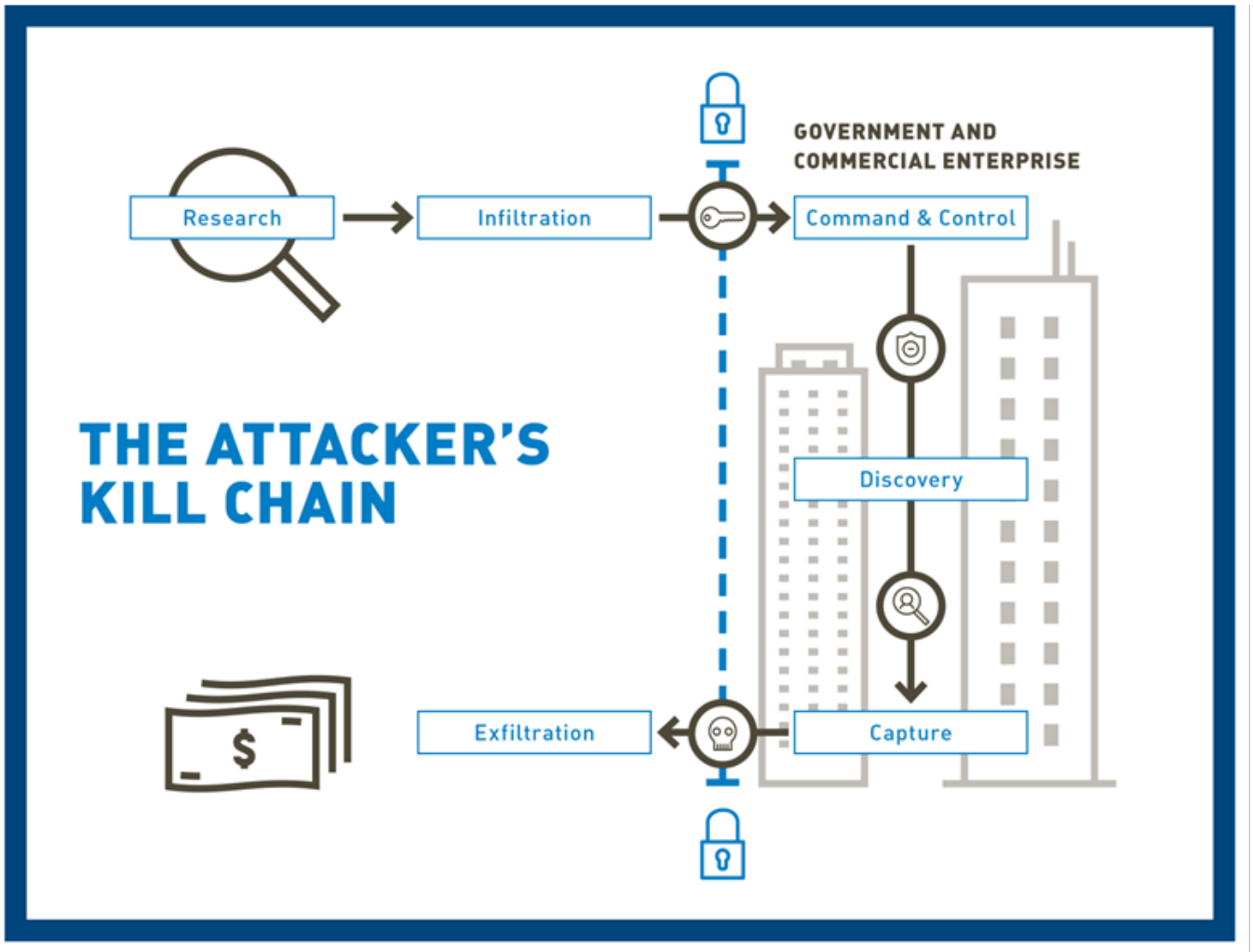
Infiltration and Initial Exploit – This is the principle attack vector that is used to successfully gain a foothold within the target system.

Callback, Download and Set-Up of Command and Control – The initial exploit is simply about gaining a foothold. Once this is done, the initial exploit will communicate home and then will download additional tools and instructions. These stage 2 payloads are typically more sophisticated and targeted.

Discovery and Lateral Expansion – The attacker rarely has intimate knowledge of the target environment, therefore they have to map the network to identify additional targets and resources. Traditional cyber security tools tend to focus mostly on the perimeter and hosts, often missing this unusual behavior. The attacker is never satisfied simply controlling the initially compromised system. They could be discovered at any time, or the system could be moved or shutdown. They will move laterally throughout the network as rapidly as possible, compromising other systems to give them multiple points of access if one becomes unavailable. This lateral movement will also bring them closer to the best target data.

Data Collection – Once the target data is identified, it is either collected locally on the target system or consolidated somewhere on the internal network. The attacker often uses either methodology based on their specific preferences. If consolidated, it becomes simpler to package and ship the data all at once. If left decentralized, it may be easier to disguise the exfiltration as legitimate traffic.

Exfiltration – As the attacker gains access to the target data, next it must be moved off network. This means opening up outbound connections and moving the sensitive data. The attacker will do everything it can to disguise the data exfiltration as legitimate traffic. With today's ubiquitous use of SSL and other encryption services, it becomes very difficult for traditional perimeter tools to identify the theft of sensitive data.

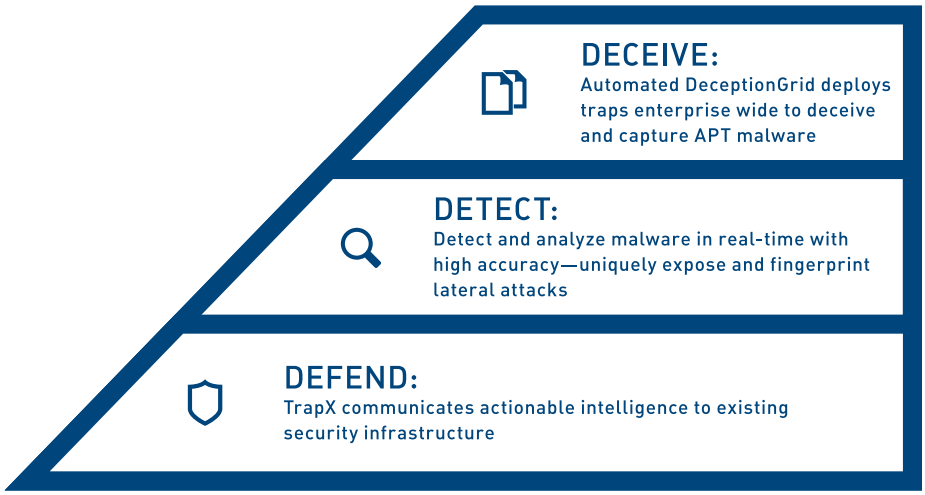


INTRODUCING DECEPTIONGRID™

Deception technology is a new category of cyber security designed to meet head-on the threats of malicious software, targeted attacks, zero day exploits and other sophisticated attacks. DeceptionGrid automates the deployment of a network of camouflaged malware traps that are intermingled with your real information technology resources. The traps appear identical in every way to your real IT assets.

Once malware has penetrated your enterprise, the attackers move laterally to find high value targets. Just one touch of the DeceptionGrid sets off a high confidence ALERT. Real-time automation isolates the malware and delivers a comprehensive assessment directly to your SOC team.

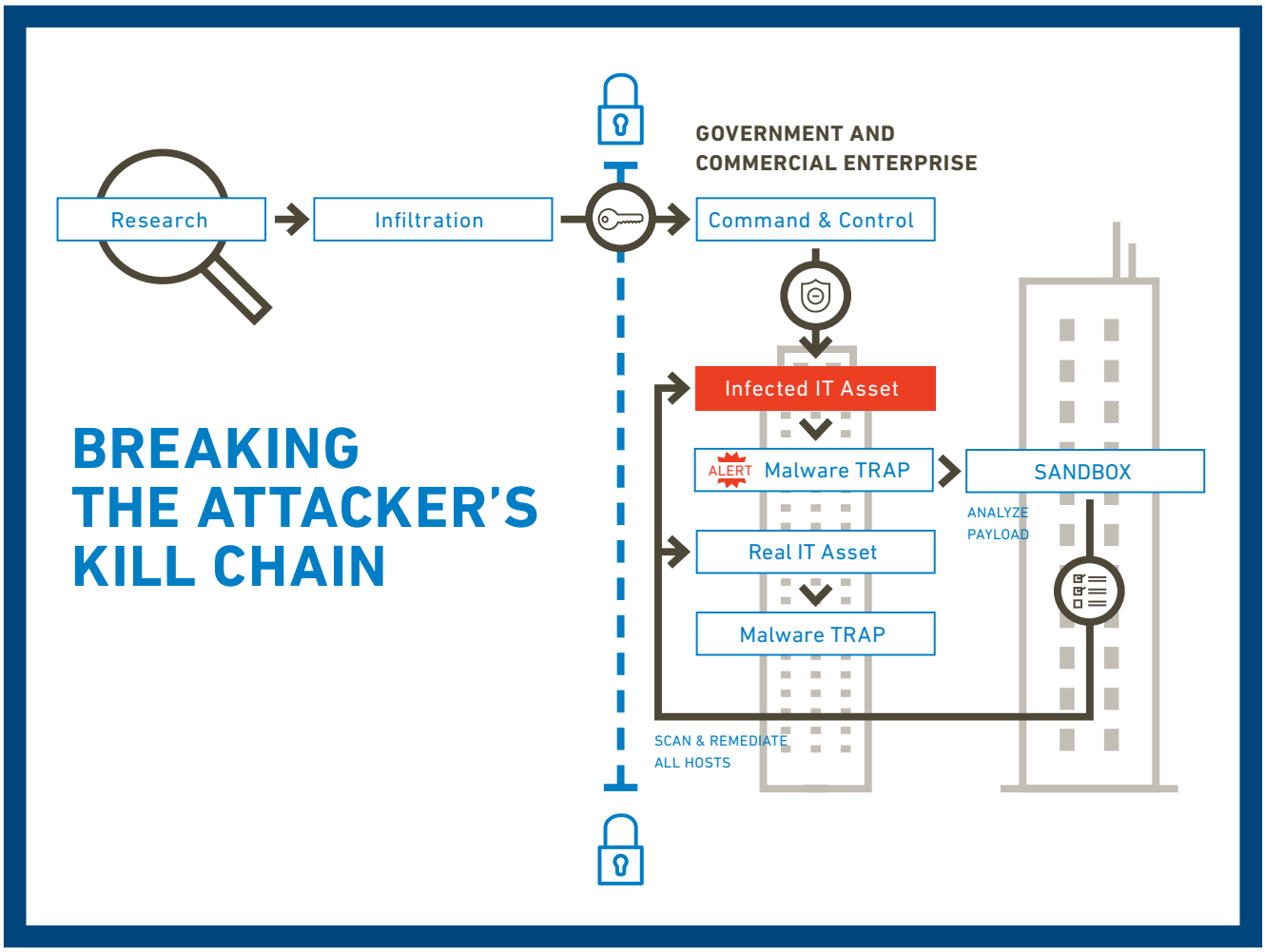
DeceptionGrid™



Now the basic pattern of malware deployment and privilege escalation activity is disrupted. At the first moment of reconnaissance and lateral movement the APT is identified positively. Automation adds powerful forensics so that your SOC team has an almost immediate understanding of the nature of the attack. You can begin rapidly to implement the best path for remediation and removal.

DeceptionGrid – Breaking the Intrusion Kill Chain

The TrapX DeceptionGrid™ now makes it possible break the intrusion kill chain. Attackers map the network and move laterally. Just one touch of the DeceptionGrid sets off a high confidence ALERT. Real-time automation isolates the malware and delivers a comprehensive assessment directly to your SOC team.



DeceptionGrid – Core Functionality

DeceptionGrid has been designed from the beginning to fit efficiently and securely into MSSP operations. DeceptionGrid includes Malware Trap Sensors and Network Intelligence Sensors. Our Security Intelligence Management provides Integrated Event Management and fully automated Forensic Analysis.

This automated analysis enables the SOC to move faster yet at the same time reduce costs as excess escalation is no longer required. Further, DeceptionGrid's mechanism of generating an alert is not based upon a probabilistic event or clustering around adjustable thresholds. These are very high confidence events. These alerts are directly generated and triggered by explicit contact with our Malware Trap Sensors.

DeceptionGrid includes important core functionality to support your cyber defense. This includes:

Automated Deployment of Camouflaged Malware Traps

The platform scans the existing network and creates a camouflaged network of emulated systems, including servers, switches, databases, and applications, interleaved with the real assets.

Sandbox Analysis

Payloads affecting these malware traps are immediately inspected for known behaviors, such as a search engine crawler, and any unknown activity is transferred and isolated in a sandbox server. As soon as Zero-Day malware starts executing within the sandbox, the platform's forensics server examines it and builds a detailed model of the exploit architecture in real time, with no added expertise needed from security personnel. This radically reduces the time and effort required to identify, analyze, and remediate threats. DeceptionGrid produces a level 3 analysis. This includes both a static and dynamic analysis, profile and signature set.

Integrated Event Management

The information produced in this automated analysis is then pulled into the platform's management system, tagged with a distinct event ID, and stored within an integrated event- management database. This actionable threat intelligence can be shared or integrated with customer's existing security systems in the network.

Threat Intelligence

DeceptionGrid's business-intelligence engine builds a profile of the attack vector and performs root-cause analysis on the event. The engine then correlates this information with outside information from a fully integrated threat-intelligence feed.

Outbound Packet Inspection (BOTNET Detection)

DeceptionGrid also provides packet inspection of outbound traffic to identify malicious behavior on existing servers. DeceptionGrid uses intelligence from the malware traps to target specific behaviors and components, and to spot lateral movement of complex threats. This sharing allows the engine to catch more infected assets before they spread. This sharing also adds greater scalability and efficiency to the system, and avoids many of the performance and latency problems associated with deep packet inspection technology.

DeceptionGrid – Key Components

These are the key components in a system deployment:

Malware Traps

A mesh of virtual decoy malware traps lure and divert APT and Zero-Day attacks away from real hosts. This grid of decoy malware traps runs low-level emulations of many real-life systems in the network to present attackers with a high-fidelity emulation of reality. Our virtual network of malware traps undetected Zero-Day malware before it can infect real IT assets.

Management Dashboard

A dashboard with fully featured sandbox capabilities allows payloads captured by DeceptionGrid sensors to execute for real-time forensics investigation. An automated forensics engine examines payload as it executes in real time within the sandbox to identify and catalogue unique behavior and attributes of Zero-Day activity. Event data is pulled into a comprehensive event management database.

Business Intelligence Engine

A business intelligence engine takes event data and builds profiles to detect and prevent future attacks. A threat intelligence feed layered into event analysis is integrated directly into the management system, enabling the attribution and creation of topology maps. This rich data and intelligence analysis allows for swift remediation of known attacks against IT systems.

DeceptionGrid Platform

Users can deploy the TrapX platform in the cloud or on their premises. The platform is fully integrated and extensible. All communications between sensors and the management platform are secured by an encryption protocol that allows real-time updates without any kind of inbound firewall connection.

"Detection is a binary event – not probabilistic. There is no cloaking available to APTs that enables them to violate the integrity of the detection. There are no false alerts. Any cyber event that touches the interlaced network of virtual "decoy" computing resources in DeceptionGrid is by definition malicious and unauthorized activity and immediately alerted to your SOC."

Yuval Malachi
Chief Technology Officer, TrapX

DeceptionGrid Benefits and Value

Deception technology brings strong benefits to our customers. We address key pain points within their existing cyber defense strategy.

Some key value points include:

- Uniquely, we detect mid-point VLAN movement by malware in real-time which is unseen by other cyber defense. We monitor and protect these areas. This ultimately reduces the risk of economic loss, impact to business operations and loss of intellectual property.

- Uniquely, our technology detects the movement of advanced malware almost immediately. We dramatically reduce the time to breach detection for the most sophisticated zero day events, advanced persistent threats (APTs) and other malware. The longer an attacker has access to your internal networks the greater the probability of severe economic and operational impact. Reduction in time to breach detection is a critical and important metric.

- Uniquely, we generate a small number of highly accurate and actionable alerts. Important events are not missed or ignored by your security operations command (SOC) team. This reduces the risk as you can now more rapidly detect and defend against these complex threats. No big data, no need to process thousands or millions of alerts. And no missed alerts.

- Uniquely, when we identify malware within the VLAN we automatically deliver a complete static and dynamic analysis. This provides your SOC team with a complete level 3 analysis without extensive manual processes. This helps reduce the time for your SOC team to determine appropriate action.

- Our deployment is automated, simple and very fast. Our automation reduces the investment required to protect the entire enterprise. This makes it easy to plan for rapid deployment.

- Our Threat Intelligence Center automatically flows information from discovered threats across our network so that our customers can immediately benefit.

- DeceptionGrid seamlessly integrates into your existing network architecture without requiring any changes to configuration or topology. This saves time and resources upon the initial implementation and over the life cycle of system support.

ABOUT TRAPX SECURITY

TrapX Security is a leader in the delivery of deception based cyber security defense. Our solutions enable our customers to rapidly isolate, fingerprint and disable new zero day attacks and APTs in real-time. Uniquely our automation, innovative protection for your core and extreme accuracy enable us to provide complete and deep insight into malware and malicious activity unseen by other types of cyber defense. TrapX Security has many thousands of government and Global 2000 users around the world, servicing customers in defense, healthcare, finance, energy, consumer products and other key industries.

Find Out More – Download a Free Trial

Come to www.trapx.com and download our FREE proof of concept and trial for qualifying organizations.

Find Out More – Contact Us Now

TrapX Security, Inc., 1875 S. Grant St., Suite 570 San Mateo, CA 94402
+1–855–249–4453
www.trapx.com

For sales: sales@trapx.com
For partners: partners@trapx.com
For support: support@trapx.com

Trademarks