LOOKINGGLASS

ENDING ABSURD CHESS

MITIGATING CYBER ATTACKS WITH THREAT INTELLIGENCE, INTEGRATION, AND AUTOMATION

CONTENT

INTRODUCTION: ABSURD CHESS

Imagine a prestigious international chess tournament with the following gameplay rules:

1. While opponents will play games on the same board, this board will not be completely visible to either player at all times. Even when visible to one or both players, the board may not completely and accurately reflect the current state of the game.
2. At no time during any game will players be provided with real-time updates on the opponent's last move. To the degree updates are given, a player will not know how many moves have occurred since.
3. Each player will be provided with a full set of chess pieces, but the tournament requires a team approach. Teams are comprised of strangers, wherein one person plays all pawn moves, another person plays knights and bishops, someone else plays rooks, and the captain plays only the queen and king.
4. During gameplay, teams may or may not be able to communicate and coordinate the game plan. This means, at times, teammates will play their respective pieces without regard to what other teammates or the opponent is doing.

This may sound like an absurd chess tournament, but many security teams try to defend enterprise networks exactly this way. Consider the parallels between the rules of the absurd chess tournament outlined above and the following operating principles of many security teams today, which correlate respectively (e.g., Rule 1. above to Operating Principle 1. below, etc.):

1. Many enterprise security teams do not have full visibility of what is occurring on their own networks. From shadow IT [1] and an absence of database monitoring [2] to lax identity and access control management (IAM), much legitimate activity is not visible. Of course, this says nothing of malicious activity. Trying to secure a network this way is akin to playing chess on a board that does not reflect the current state of the game and is only partially visible.
2. Many security teams attempt to defend their networks without real-time threat intelligence. Threat intelligence provides information on the behavior of threat actors. Real-time threat intelligence is important because threat actors rapidly evolve methods, and threats are polymorphic. Without timely threat intelligence, security becomes like playing chess without knowledge of the opponent's last move. How can security teams possibly react properly?
3. Many security teams today take a "Frankenstein" approach to security architecture. They buy firewalls from this vendor, web proxies from that vendor, and intrusion detection/prevention systems (IDPS) from yet another vendor. The end is predictable: A monster of an architecture to deploy, configure, and maintain.
4. Once security teams have created their monster, the next challenge is to coordinate the disparate parts into a unified and dynamic defense. This requires integration, so the parts "talk" to one another. But many vendors build products designed not to communicate or work with other vendors' products. While some achieve integration, it proves to be largely futile if internal teams don't have the tools to work effectively together. This common scenario is further complicated because teams can't see all of their own networks (1.) and don't have timely intelligence to communicate (2.). In the end, for all the complexity the Frankenstein approach creates, the capabilities are not additive.

Surely there's a better way to approach security than like an absurd game of chess.

ELEMENTS MISSING FROM TODAY'S SECURITY STRATEGIES

In theory, traditional security devices (e.g., firewalls, web proxies, etc.) and techniques (e.g., access control, account management, etc.) work. The steady parade of headlines announcing compromises and data breaches suggests that, in practice, these defenses are incomplete. In some cases, the elements are in place, but something is missing in how they work together to form an effective defense.

The information technology and advisory Gartner has identified "adaptive security" as a major industry trend going forward. [3] Threat intelligence is central to an adaptive security model, as Gartner explains:

"An intelligence-driven security operations center (SOC) goes beyond preventative technologies and the perimeter, and events-based monitoring. An intelligence-driven SOC has to be built for intelligence, and used to inform every aspect of security operations. To meet the challenges of the new 'detection and response' paradigm, an intelligence-driven SOC also needs to move beyond traditional defenses, with an adaptive architecture and context-aware components. To support these required changes in information security programs, the traditional SOC must evolve to become the intelligence-driven SOC (ISOC) with automation and orchestration of SOC processes being a key enabler." [3]

To become more adaptive, security teams must have better information, establish more coordination between teams and devices, and more quickly deploy effective mitigation techniques. Such a model requires key elements that are missing from many of today's security operations and which include the following:

Actionable threat intelligence – Threat intelligence provides visibility into what is happening on enterprise networks, as well as emerging threats on external networks. Without timely and accurate threat intelligence, security teams have no visibility into the tools, techniques, and procedures (TTP) being used by threat actors. The absence of quality threat intelligence reduces security to mere guesswork. There is certainly no adaptation, and how can there be when there is no information to use in adapting defenses?

Integrated security architectures – To be effective, threat intelligence must be the basis for specific defenses. For instance, threat intelligence on a malicious Internet Protocol (IP) address/domain name must be implemented into firewalls, web proxies, and IDPS. The configuration of any device in isolation must not conflict with any other device. They must work in concert to achieve defense in depth. Likewise, teams must work in collaboration and constantly communicate. Without intelligence and integration, the smartest security teams using the best security devices in the world make for a "dumb" defense.

Automated mitigation responses – A key challenge for today's security teams is the sheer number of alerts and potential incidents that must be reviewed, verified, and then mitigated – if found to be legitimate. Human security teams are overwhelmed, and this creates a natural gap between the time a threat/attack is detected and the time a team takes action to mitigate it. A recent report said that attackers remained undetected on enterprise networks 146 days (median) in 2015 – a decrease from the 2014 median of 205 days. [4] Part of the solution is to partially automate mitigation by feeding intelligence directly to security devices, which can then automatically act on the intelligence to block threats.

In addition, security teams sometimes get married to tools that don't allow for optimal use of high-quality intelligence. Teams must plan the steps for effective responses given specific types of intelligence.

An increasingly critical element in an effective defense is the ability of security tools to remain undetectable to attackers and malware. The nearby case study details just one recent example of how sophisticated malware has become in subverting standard security measures.

Together, these elements – intelligence, integration, and automation – form the basis for what LookingGlass calls Dynamic Threat Defense.

Case Study: Furtim Malware

Attackers and the malware they develop continue to exhibit increasing levels of sophistication. In July 2016, security researchers discovered yet another example in the so-called Furtim malware. Furtim was discovered on an underground forum known for facilitating a malware marketplace. [5] Upon further investigation, the researchers found the malware installed on at least one European electric utility. [6]

Like other advanced malware, Furtim was designed to be a multistep exploit. The initial "dropper" is installed on a machine and is programmed to immediately identify the presence of sandboxes, which execute code in isolation from the machine's operating system (OS) in order to detect and prevent malware from downloading to the computer's critical OS (physical or virtual). The dropper is also programmed to identify honeypots, which are devices purposely set up by researchers to lure attackers and malware in order to identify and study them in a controlled environment.

These capabilities are not unique to Furtim, but the next phase of compromise is remarkable. According to researchers, Furtim is designed to identify the presence of antivirus software on a machine and then to systematically disable it – process by process – until the antivirus program can be uninstalled. [6] Once the antivirus is removed, Furtim prohibits easy re-installation, and even if successful, the antivirus is prohibited from receiving virus signature updates and software upgrades. [5]

Furtim then remains invisible to system administrators and provides attackers with an established backdoor through which to access and map the network, as well as to issue commands from a remote server. [6]

Without timely and quality threat intelligence, integration of security devices, and automated mitigation, such an attack could persist for as long as the attackers deemed necessary, and the enterprise security team may never know that anything is awry.

THE LOOKINGGLASS APPROACH TO THREAT MITIGATION: INTELLIGENCE, INTEGRATION, AND AUTOMATION

LookingGlass offers a solution portfolio that operationalizes threat intelligence and provides automation to block all threats, including critical ones targeting the organization. The products offer a high level of security and sophistication, preventing attackers from recognizing that they are being detected. They are fully integrated with actionable threat intelligence that originates from high-quality data feeds, allowing for automated mitigation at machine speeds.

The foundation of LookingGlass's threat mitigation approach is deep packet processing (DPP), which is achieved via the Deep Packet Processing Module (DPPM) – a purpose-build hardware specifically designed to enable DPP. As the name suggests, DPP goes beyond merely inspecting packets and actually processes packets in-line at speeds up to 30 million packets per second.

DPP – which separates the forwarding and control planes in networking devices such as switches and routers – inspects, forwards, drops, clones, and/or modifies data at the application

layer (i.e., Layer 7 in the standard Transmission Control Protocol/Internet Protocol [TCP/IP] model). Through the use of "accelerator" technology, DPP works with no noticeable latency (< 10 µs). Because the packets are interpreted, rather than executed, in the environment, DPP detects malicious payloads without exposing assets to their effects (e.g., infection).

DPP is available on two platforms – the CS-4000E and the CS-4000. These appliances are often arranged at the perimeter of enterprise networks to filter all inbound and outbound traffic. The CS appliances themselves are designed to eliminate common threats on standard servers. For instance, the CS platform is diskless, possesses no insecure ports or drives, and encrypts internal/external management communications. In addition, DPPM possesses no IP or media access control (MAC) address, providing no network presence and therefore making it invisible to attackers. Appliance integration requires no changes to the existing network.

In combination with policies and/or programming, DPP does not merely block or copy packets – it modifies the payload in-line, reducing the lag time between threat identification and required mitigating action to milliseconds.

The CS appliances integrate with three other products in the LookingGlass portfolio to provide a technological foundation for Dynamic Threat Defense, including life-cycle threat mitigation via intelligence, integration, and automation.

NetDefender

What It Does: Integrates malware defenses by gathering threat intelligence from malware sensors (including rules created by LookingGlass and third-party products) and using this information to automatically update rules used by CS-4000 and CS-4000E appliances.

The CS-4000 products are usually placed near the network perimeter in order to filter all inbound and outbound network traffic using DPP. Once CS appliances receive updated threat intelligence, their DPP rules will automatically begin blocking malicious payloads. This eliminates the lag time often present between machine detection of malware and the required human action to implement safeguards.

NetDefender separates traffic handling from the control plane. This separation enables custom programming to be applied at the data plane for application packet inspection and traffic routing, as well as at the control plane for automation and orchestration of provisioning and configuration. Since data inspection happens in-line, packets are not required to be routed through expensive and hard-to-maintain out-of-path sensors. This simultaneously satisfies network engineers' security requirements and network architects' availability requirements.

Through NetDefender's Control Plane application programming interface (API), sensors can be automatically updated to block the most urgent threats. NetDefender's graphical user interface (GUI) allows human analysts to define traffic steering and manually manage threat mitigation policies.

How It Enables Dynamic Threat Defense: NetDefender provides the following:

- **Intelligence** sourced from LookingGlass Threat Intelligence Platforms.
- **Integration** with CS-4000 appliances and threat intelligence platforms, as well as third-party malware sensors.
- **Automation** via the ability to program automatic blocking, based on real-time threat intelligence, as well as policies for traffic steering.

DNS Defender

What It Does: DNS Defender is a purpose-build threat mitigation appliance that protects against DNS attacks, accelerates DNS performance, and prevents malware from using internal recursive domain name servers (DNS) to establish communication with the malware's command and control (C2) server.

Increasingly, malware attacks contain multiple steps. The first step usually involves installing a "dropper," which is a lightweight program that infects the device but does not contain the main

payload. Once installed, the malware collects information on the host machine (refer back to the case study for an advanced example of this) and then tries to establish a connection to remote C2 servers. These servers host the main payload and, through remote communication, can issue commands and execute code on the compromised device. Hackers frequently use the DNS protocol to communicate with C2 servers because traditional firewalls usually allow legitimate DNS traffic, giving attackers access and cover.

DNS Defender is a purpose-built firewall specifically for DNS traffic. While traditional firewalls support DNS application inspection, the sheer volume of DNS traffic warrants a specific, purpose-built firewall. DNS Defender prevents malware from communicating with its host C2 servers by blocking malicious IP addresses/domain names. The list of malicious C2 servers is constantly updated by LookingGlass's VirusTracker, which provides raw threat intelligence to DNS Defender via real-time data feeds. Virus Tracker identifies, on average, 65,000 new malicious IP addresses/domain names every week.

DNS Defender is a protocol-specific DNS firewall. Protection includes prevention of popular distributed denial of service (DDoS) amplification attacks, which rely on the ability to direct high volumes of traffic from unprotected open DNS recursive servers to a target.

How It Enables Dynamic Threat Defense: DNS Defender provides the following:

- **Intelligence** sourced from LookingGlass Threat Intelligence Platforms.
- **Integration** with CS-4000 appliances and threat intelligence platforms, as well as internal recursive DNS servers.
- **Automation** via traffic blocking at all seven layers of the TCP/IP stack.

NetSentry

What It Does: Provides an enterprise-grade network IDS. It contains two primary elements: (1) An optimized implementation of the open-source software Snort; and (2) the central processing unit (CPU) power and parallelism available with multicore technology on LookingGlass Content Processing Accelerator (CPA) modules.

Importantly, if set up alongside a DPP module, then NetSentry sensors become invisible to attackers, which prevents specific targeting and attack.

How It Enables Dynamic Threat Defense:

- **Intelligence** sourced from Threat Intelligence Platforms.
- **Integration** with CS-4000 appliances, threat intelligence platforms, and the open-source IDPS Snort.
- **Automation** via blocking of known threats.

Ending Absurd Chess with Dynamic Threat Defense

A chess match is a natural analogy for cyber security. Yet the self-imposed operating principles of many security organizations today result in a sort of absurd ruleset. This would be – and has been, for many – perilous enough in a "standard" match, but given the number of cyber risks, threats, and attacks, as well as how quickly they are evolving, the strategy is no longer effective.

Gartner says security must become adaptive to remain effective. LookingGlass provides the technological basis for adaptive security through Dynamic Threat Defense. Dynamic Threat Defense combines three elements:

1. Timely and accurate threat intelligence
2. Integration of security products and teams
3. Automation to decrease the lag between threat identification and mitigating action

Threat mitigation via Dynamic Threat Defense is one key piece in the threat intelligence life cycle:

1. Acquiring
2. Aggregating
3. Actioning

For more, read the white paper on Machine Readable Threat Intelligence and Threat Intelligence Platform. Learn more by visiting LookingGlass.

ABOUT LOOKINGGLASS CYBER SOLUTIONS

LookingGlass delivers the most comprehensive threat intelligence-driven solutions in the market, enabling security teams to efficiently and effectively address threats throughout the cyber threat life cycle.

With a scalable solutions portfolio of threat data feeds, a threat intelligence management platform, threat mitigation solutions, and threat intelligence services, LookingGlass enables security teams to prevent, detect, understand, and respond to analyzed, prioritized, relevant threats.

Additionally, with a deep knowledge of the global Internet topology and near real-time activity, LookingGlass helps organizations understand threats inside and outside their perimeter – including threats that may be impacting third party trusted partners, other organizations in their industry, and the latest threat trends impacting the global Internet at large.

Know More. Risk Less.

REFERENCES

1. Muncaster, Phil (July 19, 2016). "Over One-Third of Managers Would Bypass IT Security." Info Security Magazine. <http://www.infosecurity-magazine.com/news/over-one-third-of-managers-bypass/>
2. Chickowski, Ericka (April, 21, 2016). "Databases remain soft underbelly of cybersecurity." Dark Reading. <http://www.darkreading.com/application-security/database-security/databases-remain-soft-underbelly-of-cybersecurity/d/d-id/1325216?>
3. Gartner (June 15, 2016). "Gartner Identifies the Top 10 Technologies for Information Security in 2016." Gartner Newsroom. <https://www.gartner.com/newsroom/id/3347717>
4. Lennon, Mike (February 25, 2016). "Breach Detection Time Improves, Destructive Attacks Rise: FireEye." Security Week. <http://www.securityweek.com/breach-detection-time-improves-destructive-attacks-rise-fireeye>
5. Franceschi-Bicchierai, Lorenzo (July 12, 2016). "Researchers Found a Hacking Tool that Targets Energy Grids on the Dark Web." Motherboard. <https://motherboard.vice.com/read/researchers-found-a-hacking-tool-that-targets-energy-grids-on-dark-web-forum?utm_source=Sailthru&utm_medium=email&utm_campaign=Defense%20EBB%2007-13-16&utm_term=Editorial%20-%20Early%20Bird%20Brief>
6. Goodin, Dan (July 12, 2016). "Nation-backed malware that infected energy firm is 1 of 2016's sneakiest." Ars Technica. <http://arstechnica.com/security/2016/07/nation-backed-malware-that-infected-energy-firm-is-1-of-2016s-sneakiest/>