CRYPTONITE NXT

The smarter way to defend your network

An overview of cyber security problems in today's networks and CryptoniteNXT's innovative approach to securing them.

"Attackers currently enjoy unconstrained time to operate. Their campaigns, which often take advantage of known vulnerabilities that organizations and end users could have—and should have—known about and addressed, can remain active and undetected for days, months, or even longer."

THE CISCO 2016
MIDYEAR SECURITY REPORT

Introduction

The balance of power in the cyber security war is a function of time and space. Currently, the criminals have enough of both to succeed in almost any enterprise. They can hide in stealth mode, take the time to conduct reconnaissance on the network and move around with freedom exploiting critical resources. Organizations become permanently damaged even before cyber analysts detect the breach. Financially motivated attackers take the path of least resistance to achieve their monetary goals. Nation State attackers use more sophisticated tools and strategies and are giving us a glimpse into the future of cyberattacks.

Enterprise networks were not designed with the notion of security but instead to provide maximum connectivity, ease of use and maximum performance. This mindset has created a situation where attackers have the advantage and defenders are in a constant race against time to detect, mitigate, and recover from a continuous stream of new attacks.

As a result, networks are falling victim to "death by a thousand cuts." While the endeavor of neutralizing each item in the attacker's bag of tricks is worthwhile, it is time to rethink the parameters of the war. A new paradigm is needed that will enable the network to protect itself and shift the balance of power back to the enterprise. What is needed is to deploy defense mechanisms that create permanent, fundamental disruptions in the attacker's tactics. Such a proactive network must constantly defend itself against known and unknown attacks. A proactive network must also force the attacker to become reckless thereby exposing himself and aiding quicker detection. The network can do so by concealing any information that can be used to effectively plan an attack, constraining the breadth and depth of network reach from any single point, validating network actions as they occur, and applying tight controls to contain the spread of an attack, all without the need for human intervention. This is the smarter way to defend your network.

This white paper describes CryptoniteNXT, an innovative strategy in cyber defense. CryptoniteNXT is not another offering attempting to detect compromises after critical information has been stolen. It is a tool that strengthens the security posture of the network by stopping attackers from gaining access to network resources and containing malicious actors that have entered the network, giving modern day cyber security detection tools something that they currently do not have - time to detect. CryptoniteNXT combines two enabling technologies—moving target defense and software-defined segmentation—to disrupt an attacker's tactics and eliminate the advantages that enabled network compromises. CryptoniteNXT stops attacks by concealing information about the network, shielding from unnecessary exposure, and proactively defending the network before detection. This whitepaper describes how CryptoniteNXT defends your network before detection using example malicious activities such as reconnaissance, ransomware, and insider threats.

"If you really want to protect your network, you really have to know your network. A targeted intrusion starts with Reconnaissance."

ROB JOYCE,
TAILORED ACCESS OPERATIONS,
NSA

The How and Why of Cybersecurity Problems

Today's attackers use tactics honed over many years to take advantage of fundamental design flaws in network technology. While the specifics vary daily, the modus operandi remains consistent.

Anatomy of an Attack

An attack follows one or more phases in a kill chain, the basic steps a malicious attacker takes during an intrusion. Each phase is dependent on the success of the previous one.

Reconnaissance, Weaponization and Delivery of Malware

To aid attack planning and avoid detection, the attacker begins with reconnaissance. The goal is to gain a foothold in the network, enumerate reachable devices, and find ways to move laterally. Techniques used to gain entry include social engineering, physically observing an office building, and mapping the network from external sources. Once the attacker has gained a foothold within the network, it can also be used as a launching point for further network-based reconnaissance such as full and undetected scans of the network. A single compromised computer can spoof arbitrary servers undetected, collecting credentials and other critical information to rapidly focus the attack.

Exploitation, Installation and Command & Control

By now, the attacker has determined which systems possess known vulnerabilities, how to access them and has formulated a comprehensive attack plan. Whether through encrypted command and control channels or embedding information into malware, the attacker then moves laterally to deliver the malware to critical resources and compromise the rest of the network. The attacker can move easily within the interior of the network, away from the prying eyes of perimeter-based firewalls and detection systems.

A combination of stolen credentials, inconsistent network configurations, systems configuration errors, and software vulnerabilities all but guarantee success in this stage of the attack.

Actions on Objective

The attacker can then quickly and efficiently execute their objective, for example exfiltrating sensitive data, holding the entire network hostage for a ransom, or inflicting other damage on the enterprise. The entire attack process takes just a few hours or days. Once the majority of the network is compromised, software-based protection (anti-virus, host-based IDS, etc.) can be rendered inoperable by a sophisticated attacker. State-of-the-art detection and management systems require humans to deploy patches, investigate alerts, and take action. The result is that infected systems often fester for months before detection.

"Protect the rest of your network from compromised desktops and laptops by segmenting the network and implementing strong authentication."

VERIZON 2016 DATA BREACH INVESTIGATIONS REPORT

Why are Networks Insecure?

To address the problem, it must first be precisely identified. The crux of the problem is that today's networking technologies were built with a false reliance on trust. Many of the TCP/IP based protocols and software that provide the foundation for networks were designed for openness, cooperation and standardization. This philosophy produced the explosive growth of information technology, interconnected the world in unprecedented ways and produced exponential gains in productivity across all industries. However, these very same qualities have now become detrimental to network security because it affords malicious actors the same advantages in their criminal activities. Today's insecure TCP/IP-based network architectures are:

- **Static and easily discoverable**, enabling an attacker to arm himself with every detail of the network and the endpoints connected to it. An endpoint is an internet-capable device on an IP network.
- **Transparent**, because by design networks ask and respond to questions such as "who are you" and "where is this server." It is currently difficult to answer these questions in a trusted way that prevents network misuse while maintaining interoperability. Exploiting this transparency allows a variety of ways to gain access within the network.
- **Lacking controls**, because malicious actions are blocked only at the perimeter of a network, at vulnerable endpoints, or using haphazard disconnected rules. Unchecked lateral movement of the attacker within the network is far too easy.

These flaws are unlikely to be addressed in the foreseeable future due to the scale of networks and proliferation of current technologies.

Enterprise security today must operate in an environment unlike any foreseen at the inception of computer networks and the information technology era. Today, attackers are just as sophisticated as the technology innovators, and possess resources that in some cases may significantly exceed an enterprise's cyber security budget. An undetectable "zero-day" attack can be purchased for a few thousand to hundreds of thousands of dollars.1 The result is that attackers know about potential vulnerabilities and possess tools that exploit them even before administrators can patch their enterprise's systems. Attackers can evade even up-to-date malware detection systems.

State-of-the-art security technologies play a critical part in defending a network, but they are falling short. This lopsidedness allows attackers to continue to use essentially the same vulnerabilities and tactics on every network they come across. A network cannot be defended after the fact.

A pre-emptive, real-time, action against all attacks—known and unknown— is needed for the security technology to be effective.

"The time to compromise is almost always days or less, if not minutes or less."

VERIZON 2016 DATA BREACH INVESTIGATIONS REPORT

Key Innovations in the CryptoniteNXT Approach to Security

CryptoniteNXT is a network appliance that supplements existing network infrastructure to improve security. A unique combination of technologies effectively alters network behavior in real time with no human intervention. CryptoniteNXT blocks malicious activities while at the same time preserving performance and usability for legitimate purposes.

CryptoniteNXT has a security-first approach. The assumption that each endpoint device connected to the network could already be compromised via an undetected attacker is built into the design. Rather than leaving the entire network always connected and the doors open to the attacker, CryptoniteNXT controls whether each protected endpoint sees the rest of the network, how it perceives the network and how it operates within the network. By turning traditional trust assumptions on its head, CryptoniteNXT proactively contains an attack well before it can be detected and removed by traditional means. Network protection with CryptoniteNXT is therefore always on, checking that every packet is not exceeding necessary business functions, and limiting the attacker's ability to progress along the attack's kill chain.

"... with this device implemented and configured correctly, identification and enumeration of hosts becomes an improbable attack vector."

RAPID7,
NDEPENDENT SECURITY
ASSESSMENT

CryptoniteNXT uses the two technologies which work together to amplify network defense:

- **Moving Target Cyber Defense (MTD)** – Rather than allowing a protected endpoint or a malicious device to see the real network, CryptoniteNXT transforms the endpoint's view of the network into a dynamic, abstract structure, in effect making the once static network into a dynamic moving target. Normal legitimate traffic is unaffected by MTD. However, MTD severely restricts an attacker's ability to collect actionable information about the network or masquerade as another legitimate endpoint. Thus, MTD substantially increases the time, effort, and risk necessary to establish or maintain a presence in a network. The validity of any information garnered is also restricted to a limited period of time making it necessary for the attacker to repeatedly and aggressively perform reconnaissance. The attacker is unable to act decisively on network information and cannot spoof legitimate information. He becomes prone to mistakes making him more easily detectable by monitoring tools.
- **Software-defined Segmentation** – MTD creates a mapping from the obfuscated network to the real network, known only to CryptoniteNXT, to enable flow of traffic across the traditional network infrastructure. Software-defined Segmentation creates a decision point regarding whether a packet should be permitted through that mapping. This decision minimizes exposure and contains attacks while allowing legitimate communications to take place. At a per-user and per-service level, NXT decides at line speed whether a given packet needs to be permitted through the network. Unless absolutely necessary, the packet is not delivered to the endpoint thereby preventing malicious packets from ever reaching a protected endpoint. As with MTD, this protection is always on at every endpoint, so all traffic is protected.

By combining these two innovative technologies, CryptoniteNXT controls the flow of every packet through the protected network, malicious or not, even for endpoints traditionally within the same broadcast domain. After all, with the risk of the attacker using a new undetectable zero-day vulnerability and the knowledge that human response to an intrusion detection system alert may take hours or days, nothing can be safely allowed unfettered access to the network. CryptoniteNXT provides three defensive capabilities to protect a network from attacks.

Net Guard

CryptoniteNXT proactively guards the network by effectively concealing its topology from attackers. Reconnaissance tools are unable to identify vulnerabilities and obtain critical information needed to plan an attack— keeping the network secure, and attackers guessing.

Micro Shield

Compromises are inevitable. That's why CryptoniteNXT utilizes software- defined segmentation to contain malware and prevent it from spreading to other critical network services—even before it's detected. So, the network can be shielded from unnecessary exposure—whether from cyber criminals, insider threats, or just plain human error.

Auto Defend

An attack can be executed in just moments, and remain undetected for months. CryptoniteNXT is "always on" to defend the network proactively— even before detection—preventing reconnaissance, safeguarding critical data, defending against zero day exploits, and protecting network services from the reach of malicious actors, all without even knowing it.

Defending Against Attacker Tactics

To defend, one must understand the adversary's methods. There are four common tactics that attackers use as building blocks for sophisticated campaigns - scanning, spoofing, access misuse, and lateral movement. Stopping these tactics prevents the attacker from progressing in the kill chain. Eventually, the attacker will either fail, give up, or be detected, all before accomplishing their desired goals. Note that the use of these tactics is not new or a passing trend. These are key actions enabled by an attacker's knowledge of fundamental network security deficiencies. Stopping these tactics has a long-term impact on an attacker's ability to operate.

In a protected network, the CryptoniteNXT appliance processes each packet that passes between the network and each protected endpoint. CryptoniteNXT makes decisions about whether to permit the packet through the MTD mapping, modifies the packet in ways that obscure information from prying eyes, verifies the integrity of the packet as it traverses the network and dynamically controls the packet's path through the network. CryptoniteNXT makes scanning ineffective

Scanning is the tactic of searching the network's IP subnet to understand what IP addresses are assigned to each endpoint, determining what servers and services exist that can be impersonated, and finding which known software vulnerabilities are likely present on each endpoint. In a network protected by CryptoniteNXT, scanning produces different results every time due to MTD. All of the IP addresses seen by the attacker are fake and unusable for any communication. No network access is possible from a malicious device added to the network. Because CryptoniteNXT dynamically alters the mapping between the view seen by an endpoint and the real network, any information collected by the attacker is transient and cannot be used at a later point in time.

"We expect the next wave of ransomware to be even more pervasive and resilient. Organizations and end users should prepare now by backing up their critical data and confirming that those backups will not be susceptible to compromise."

THE CISCO 2016
MIDYEAR SECURITY REPORT

CryptoniteNXT prevents spoofing

Spoofing, a tactic where the attacker impersonates the identity of one or more legitimate endpoints in the network, is used 1) to send traffic from what appears to be a high-privilege endpoint to gain greater access to the network, and 2) to collect credentials and other information by posing as a legitimate server. CryptoniteNXT's position within the network ensures that these malicious actions are not possible. Any spoofed responses never reach the victim, and improper use of the network is blocked.

CryptoniteNXT secures access

Stolen credentials are highly valued by attackers during an attack. Bypassing or disabling defenses, such as using stolen credentials or attacking the defenses themselves, is typically the easiest way around them. CryptoniteNXT cryptographically verifies the sender's identity and the legitimacy of the requested connection. This check prevents MAC and IP address forgery and renders misuse of application or operating system credentials ineffective. Strong two-factor authentication, combined with software- defined segmentation, means security is enforced first, before packets ever reach protected endpoints. Attempts to misuse credentials, escalate privileges, and bypass network controls are ineffective in a protected network.

CryptoniteNXT restricts lateral movement

Using information gathered by scanning and credentials stolen through spoofing, an attacker can normally move from one compromised endpoint to another with ease. By moving within rather than re-entering the network, perimeter defenses may never even see the traffic and the attacker can entrench inside the network with relative ease. In a network protected by CryptoniteNXT, all traffic between protected endpoints goes through the appliance. Malicious network activity, such as malicious command and control traffic or attempts by insiders to access unauthorized services, is blocked. The network now prevents malicious exploits from ever reaching their intended recipients.

Example Attack Scenarios

CryptoniteNXT's defensive capabilities empower the network to thwart attacker tactics, enabling the network to proactively defend itself against many of the common attack scenarios. A few examples are described below. As is typical for any attack, each of these scenarios uses a combination of multiple time-tested, reliable, and effective tactics.

Scenario #1
Ransomware

Increasingly popular with attackers due to the immediate payoff from shrink-wrapped software purchased on the black market, ransomware aims to encrypt the data stored on endpoints and effectively hold the enterprise captive until a ransom is paid. The initial infection may be via an unauthorized download from a website (also referred to as a drive-by download) or from a malicious attachment in a phishing email.

Consider the case of MedStar Union Memorial Hospital which suffered a major ransomware attack in early 2016.2 The initial infection is difficult, if not impossible, for any technology, including CryptoniteNXT to prevent, if the malware uses a true zero-day exploit. After the first endpoint was compromised, the attackers used a combination of known vulnerabilities, commercially available network scanning tools, spoofing, use of stolen credentials, and unchecked lateral movement within the network to compromise the vast majority of the hospital's endpoints and render them non-functional. CryptoniteNXT stops all of these tactics. The attacker's scanning does not reveal actionable information, spoofing is not possible, stolen credentials cannot be misused, and lateral movement is contained. As a result, the ransomware can't spread beyond the originally infected computer. CryptoniteNXT turns a major uncontrolled crisis into a minor cleanup of a single computer.

Scenario #2
Reconnaissance

Attacks often start with a reconnaissance campaign that may continue for months until the attacker has collected enough information to further act. Scanning and spoofing are employed to map the network topology and steal credentials necessary to plan and execute a successful campaign against the target network. A reconnaissance scenario may also see the attacker spread malware onto other endpoints in the network when necessary to form a more complete picture, but again this increases the attacker's risk. The attacker knows that the network is unlikely to meaningfully change in the future, and the actual attack can then be carefully executed at a later time. The attacker's main concern during reconnaissance is to remain stealthy and undetected while preparing for a later and more damaging attack.

With CryptoniteNXT protecting the network, the attacker's scanning is highly restricted. The amount of obtainable information is substantially reduced and that information is not static and therefore not usable in the planning of an attack. Spoofing is completely disrupted. Failing to adapt to the changing network either during reconnaissance or when the information is later used creates easy and reliable indicators for detection of the attack. Finally, the lateral movement from one host to another is restricted, making it difficult for the attacker to understand the entire network. The attacker is left with only incomplete, abstract information with a very short shelf life.

Scenario #3
Insider Threat

The most complex and perhaps dangerous attack scenario for a network is an insider threat. Traditionally an insider threat is a rogue employee that accesses unauthorized network resources or intentionally makes them available to a separate attacker. Such a traditional insider threat has the benefit of physical access as well as non-network based ways of reconnaissance, such as company intranet pages, network diagrams, equipment purchase history, visual inspection, etc. A true insider may also effectively disable detection technologies, making defending the network prior to detection even more critical. Instead of truly coming from the inside, today's sophisticated attackers may instead trick a well-meaning employee into opening an email attachment or providing their credentials through social engineering or other means. Using this technique, any attack can easily become an "insider threat" and operate on an employee's computer using that employee's full credentials. A sophisticated attacker may also create a multi-stage command and control infrastructure where multiple other endpoints are directly or indirectly employed to bypass firewalls, jump servers, and other known internal controls.

Beyond disrupting the scanning, spoofing, and lateral movement as in previous attack scenarios, CryptoniteNXT provides the tools to prevent the misuse of credentials.

Software-defined segmentation blocks any attempts to exceed the authorized level of network access as well as the creation of complex multi-stage communication paths in the network. Packets are cryptographically verified, making it impossible to evade security controls. CryptoniteNXT enforces time-based two-factor authentication to gain access to the network. This credential-based control tightly restricts the network access to prevent unauthorized access, including that which might be used to exploit vulnerabilities or remotely control other endpoints. Malicious traffic, exploits, and attempts to gain improper access are stopped before the traffic reaches the endpoint.

Conclusion

To date, attackers have had the upper hand, possessing enough time and freedom of movement to operate within networks. In many cases, enterprises are unaware of the true state of their network's health. At the same time, by grossly overlooking the fundamental flaws in today's network technologies, the cybersecurity industry has been engaged in a futile "arms race" against attackers. Networks are facing increasingly sophisticated and aggressive attacks. With today's technologies, scanning, spoofing, misuse of credentials and lateral movement are all possible once the attacker gains a foothold in the network. Better ways to defend against common attacks and tactics must be deployed. CryptoniteNXT's moving target defense and software-defined segmentation are effective solutions against such malicious behaviors. By providing the capability to stop multiple steps in an attacker's game plan and containing compromises when they occur, CryptoniteNXT empowers the network to defend itself.

FOOTNOTES

1 Ablon, Lillian, Martin C. Libicki and Andrea A. Golay. Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar. Santa Monica, CA: RAND Corporation, 2014. http://www.rand.org/pubs/research_reports/RR610.html

2 ref: http://arstechnica.com/ security/2016/03/maryland- hospital-group-hit-by- ransomware/

For More Information

To learn more about Cryptonite, LLC and CryptoniteNXT, please email **info@cryptonitenxt.com**

This document is current as of the initial date of publication and may be changed by Cryptonite at any time.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NONINFRINGEMENT.

Cryptonite products are warranted according to the terms and conditions of the agreements under which they are provided. The client is responsible for ensuring compliance with laws and regulations applicable to it. Cryptonite does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access.

CRYPTONITE DOES NOT WARRANT THAT ITS PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

About Cryptonite, LLC

Cryptonite is a leader in moving target cyber defense. CryptoniteNXT enables any network to actively shield itself from cyber-attacks by preventing all attacker reconnaissance and lateral movement. Patent pending moving target cyber defense and micro-segmentation technologies protect enterprise networks from an advanced cyber attacker, insider threats and ransomware. The Cryptonite customer base includes leading commercial and government customers around the world. Learn more at **www.cryptonitenxt.com.**