CRYPTONITE NXT

Securing Banking and Financial Systems with Zero Trust

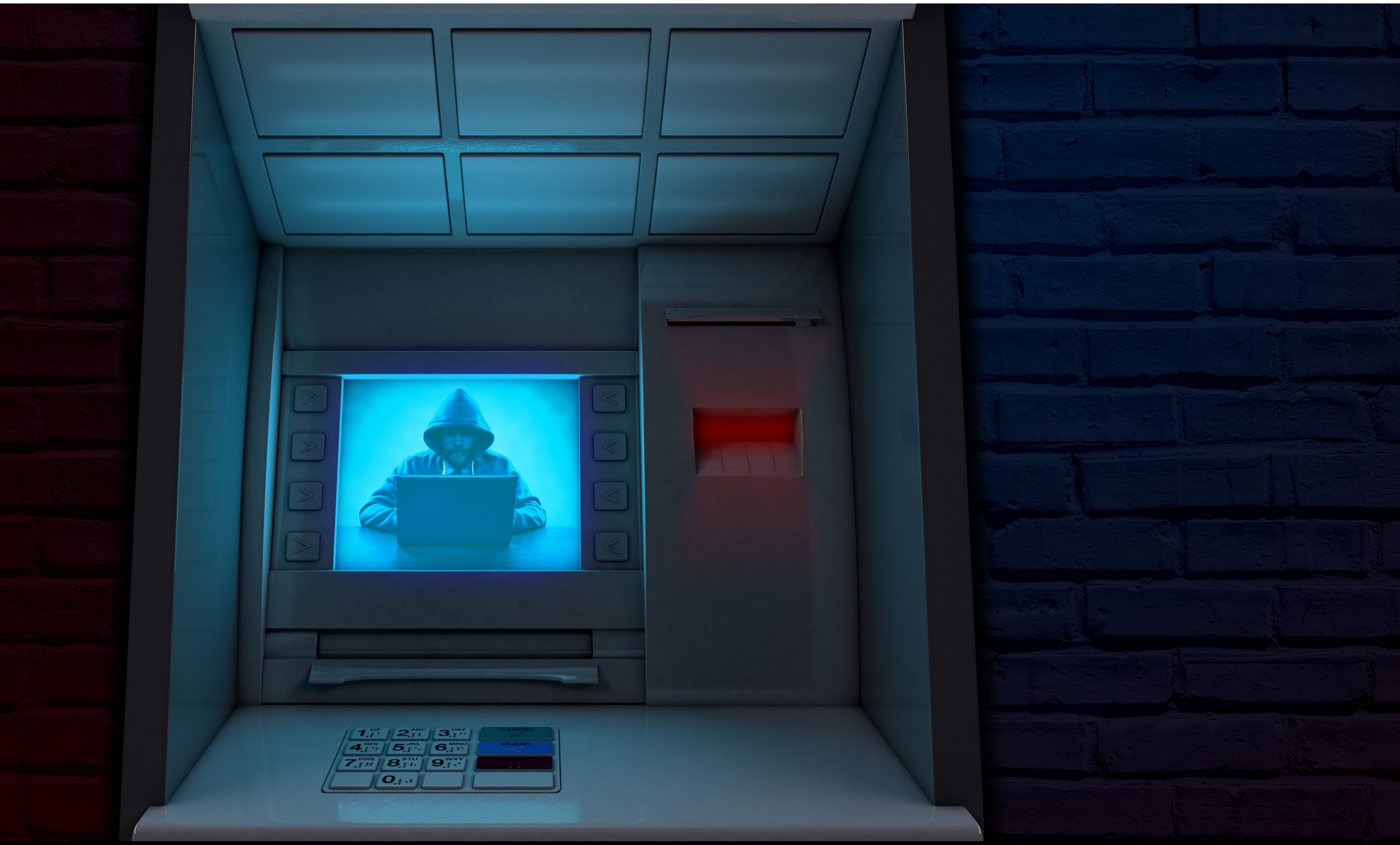
CryptoniteNXT Special Report

Contents

March 26, 2018 | This report has been sponsored by the Medical Device, Innovation, Safety & Security Consortium and Cryptonite, LLC

Notice

Cryptonite, LLC publications are made available for information purposes only. At the time of publication, all information referenced in this publication is as current and accurate as we could determine. Any additional developments or research, since publication, will not be reflected in this report. Please note that this publication may be changed, improved, or updated without notice. Cryptonite, LLC is not responsible for any errors or omissions in the content of this report or for damages arising from the use of this report under any circumstances.



Executive Summary

The financial sector has continued to sustain a rolling thunder of cyberattacks steadily since 2015. These attacks continue to target online banking, SWIFT financial systems, automated teller machine networks, and point-of-sale systems. In 2017 alone there were many hundreds of incidents, with approximately 150 involving confirmed data compromises.

Attackers' techniques, tactics, and procedures include denial of service, cyberworms, specialized financial trojans, buffer overflow attacks, brute force password crackers, point-of-sale malware, web injection, mobile device malware, spear phishing via email, social engineering, and a never-ending barrage of ransomware.

This white paper will share an overview of the many types of attacks recently experienced against banks and financial institutions, with a focus on understanding the targeted areas of vulnerability. We will include data on the evolution of the attackers and the methods they use to compromise financial networks.

Most important, we will highlight and introduce the new best practice of Zero Trust. Zero Trust technologies can substantially reduce risk, detect attacker activities early, and rapidly shut down attackers that have already penetrated your networks. We will highlight innovative technologies, such as moving target defense (MTD) and micro-segmentation, which support Zero Trust deployments. Finally, we will share our recommendations to prevent these types of attacks and to protect critical and essential financial system infrastructure.

State of the Union

Financial Industry Cyberthreats

Networks are breached directly by cyberattackers, the actions of malicious insiders, and, in many instances, unwitting participants (perhaps through misconfiguration or failure to change a default password).

The objectives of cyberattackers, usually members of organized crime, focus on financial gain. Attacks on financial institutions can provide almost immediate gratification through the diversion of funds by compromising SWIFT financial systems, online accounts, or by the theft of credit information. The compromise of automated teller machine (ATM) networks provides rapid access to cash. The sale of credit card numbers, especially for use in online transactions, remains a big business for thieves that attack point-of-sale systems.

Perhaps more disturbing to financial institutions is the strategic minority affiliated with nation-states that seek to plan the total disruption of targeted financial systems. These cyberattackers work quietly to uncover vulnerabilities and place assets to disrupt financial system operations at a future time.

Over the past few years, the volume of security events and successful attacks has increased substantially. 2015 and 2016 saw an increase in attacks, not just towards individual accounts, but directed against the banks themselves. Many sophisticated attacks have directly targeted the Society for Worldwide Interbank Financial Telecommunication (SWIFT) systems and customers. These systems are used by most major financial institutions.

The economic impact of successful cyberattacks on SWIFT systems and ATM networks is perhaps the largest of any that we have studied. For example, an attack on a bank in Bangladesh in 2016 resulted in the theft of $81 million. First, the cyberthieves used known exploits to compromise the bank's security and penetrate the networks. After reconnaissance allowed them to identify all of the servers and systems used to support SWIFT transactions, they were able to quietly observe and learn the specific workflow used by the bank to approve SWIFT transactions. Finally, the cyberthieves were able to steal high-level bank administrator credentials, which then enabled them to compromise the system and issue fraudulent transactions. In this scenario, the attacker compromised the entire network and was then able to hijack control of the trusted SWIFT network. It should be noted that the SWIFT systems were not specifically compromised - they were used normally with stolen authentication and approvals manipulated through compromised networks, endpoints, and servers within the bank.

Carbanak is one organized crime group that has targeted the banks' ATM networks directly. Carbanak is responsible for targeted attacks on over 110 banks and other financial institutions around the globe. It is estimated that these attacks have netted Carbanak close to $1 billion dollars. The Carbanak attackers start simply, by bombarding targeted banks with malware-laced emails. Once the network has been compromised, the attackers continue to exploit the Cyber Kill Chain™ through reconnaissance and lateral movement to identify resources, capture of administrator credentials, and more. Once they have the knowledge to plan and execute the attack, they can execute it rapidly and then disappear from the network systems. In many cases, Carbanak has transferred money across a global network of interlaced accounts to complete their theft. More famous, perhaps, is their success in exploiting large ATM networks such that they can direct the distribution of ATM cash, otherwise known as "jackpotting," to nearby confederates and accomplices.

Financial trojans continue to steal online banking credentials, cryptocurrency wallets, and any other account data that can be discovered. Two prominent financial trojans, Trojan.Bebloh and Trojan.Snifula, lost some momentum in 2017 as the organized criminals operating them were identified and arrested by law enforcement. Trojans such as these two were detected on hundreds of thousands of machines in 2016 and 2017. Of more recent note, a financial trojan called Emotet has recently emerged and demonstrated close to a 2,000 percent surge in activity in the final quarter of 2017. The Emotet attack is initiated through massive email distribution campaigns.

As a financial security professional, you already know that TCP/IP networks were not designed with security as the primary goal. Highly determined cyberattackers have a broad set of tools they can use to penetrate an enterprise network, bypass your cyber defense, and then move virtually unrestricted within your internal networks until they find and compromise their intended targets. It is a near certainty that a determined attacker will at some point penetrate your financial network.

→ As a financial security professional, you already know that TCP/IP networks were not designed with security as the primary goal.

Understanding Targeted Vulnerabilities in Finance

Not very long ago, cyber defense architecture consisted of little more than endpoint protection (EPP), basic firewalls, and 2-factor authentication. EPP searched for the signatures of known or probable malware such as trojans and viruses that might end up on an endpoint computer. Firewalls attempted to stop communications from known malicious IP addresses, unauthorized probes, or communication into or out of the network and more. 2-factor authentication was expensive and generally reserved for commercial banking customers.

Over time, this strategy brought in additional layered defenses to meet the increasing capabilities of cyberattackers. This includes technologies such as email filtering, various types of intrusion detection, SIEMs, and much more. Automated remediation was introduced to stop threats detected by what became an interconnected ecosystem. Firewalls gained considerable capability and reached the 2nd generation capabilities of today. Most banks and financial institutions installed software that used automation to completely reload and rebuilt endpoint operating systems once a day in an attempt to eliminate malware.

Yet, despite this increased and substantially fortified "defense-in-depth" architecture, modern cyberattackers are more successful than ever in compromising banks and financial institutions.

The strategy of defending perimeters has been the primary strategy to eliminate data breaches and theft. Given recent news and current events, it is clear that this strategy is failing. Security operations teams know that it is a certainty that at some point cyberattackers will successfully breach their networks. Attackers will successfully compromise email, entice employees through social engineering to click links to malware-laden websites, distribute infected USB memory sticks, and in some cases, enlist the support of internal malicious bad actors. Once inside the financial network, attackers have a variety of internal targets they seek to identify and a large toolkit of exploits they can use.

The perimeter has also grown softer and more vulnerable through the addition of mobile devices and the extension of new financial applications through public and private cloud infrastructure. This makes it harder to protect the enterprise and has introduced even more vulnerabilities for cyberthieves to exploit.

Given the inevitability of cyberattackers access to your internal networks, how can they be successfully detected and stopped once they are inside? The first step to answering this is to understand the vulnerabilities they seek inside of your networks and the methods they use to exploit them. Once these vulnerabilities are well defined, we can show how the deployment of Zero Trust networks can detect and automatically defeat these threats.

In banking and finance, the most highly accessible vulnerabilities include overdue software updates and patches, embedded processors in automated teller machine (ATM) networks, internet of things (IoT) devices, and point-of-sale terminals.

Overdue Software Updates and Patches

It is easier to be an attacker than a defender. Once an exploit is announced or made public, a cyberattack team can have a targeted phishing email campaign out within 24 hours to try and exploit it. Yet, even the best IT and security operations teams take a few weeks to get new updates installed. The larger the bank, in fact, the longer the internal processes required to verify, approve, and deploy the update.

Statistics suggest that unpatched software may be the #1 source of exploits for cyberattackers. According to the United States Computer Emergency Readiness Team (US-CERT) "cyberthreat actors continue to exploit unpatched software to conduct attacks against critical infrastructure organizations. As many as 85 percent of targeted attacks are preventable."

As cyberattackers perform reconnaissance within your network, they enumerate the network, determine the versions of software you are running, and then map the exploits they need to use on the identified vulnerabilities. Operating systems and applications within the network which are missing patches and updates provide an almost endless list of attack vectors for the attackers to use. Yet despite a clear understanding of the vulnerability, most teams do not keep up with required patches and updates. One reason for this is that there are just too many patches and updates. They come at enterprise software teams constantly. Each operating system and software application has hundreds of issues that need attention. Both patches and updates should be applied immediately. Industry data suggests this does not happen. Most patches and updates seem to take weeks or months to apply and, in many cases, they are never applied at all.

On top of this, information technology teams know that many patches destabilize production systems, bring new problems, and, in some cases, totally stop ongoing operations. Too many information technology practitioners have had bad personal experiences with updates bringing instability to otherwise stable systems. Some enterprise teams try to delay patch installation for a week or two in order to let someone else flush out hidden problems with the update. Then, if no major problems surface after a time, they will go ahead and roll out the updates on their own machines.

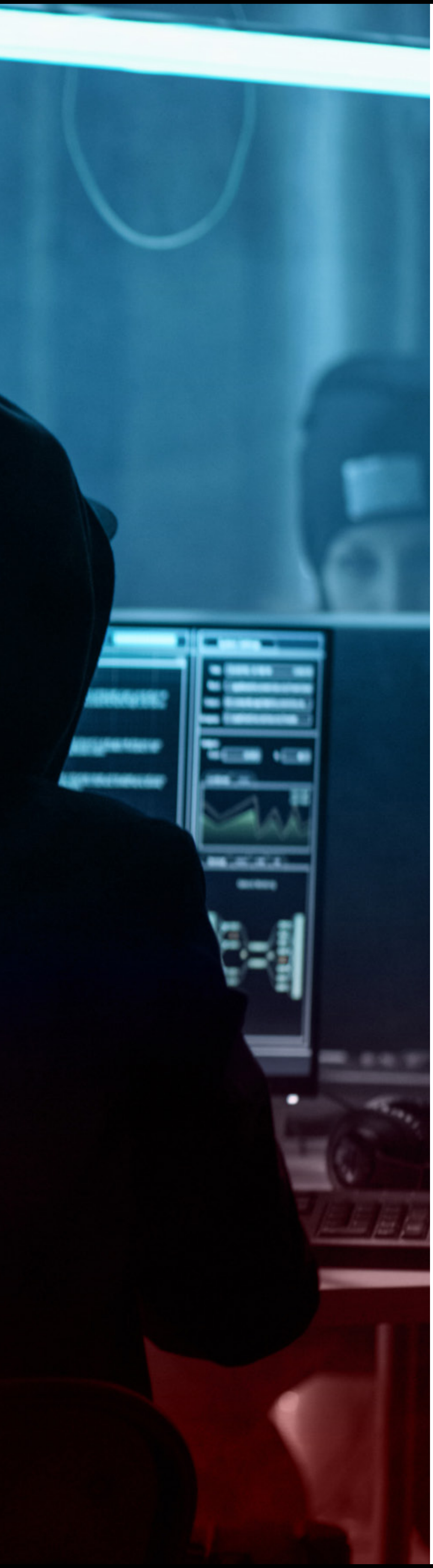
Another reason many wait is that even if the software vendor promptly issued new patches, or “fixes the fixes,” after problems are identified, it is a major pain point for those who have to uninstall the original patch and then install the new one. If you simply wait, the problematic patch may be removed from availability and replaced with one that you can install fresh without having to go through the uninstallation process.

Embedded Processors in Automated Teller Machines (ATM)

Automated teller machines represent a choice target of opportunity to cyberattackers. At present, there are approximately 1.4 million ATMs in Asia Pacific, 500,000 ATMs in North America, 800,000 ATMs in EMEA, and 290,000 ATMs in Latin America. Much of the world depends on ATMs to obtain cash, make payments, and manage deposits. Yet the embedded processors in these ATMs often have out-of-date and unpatched operating systems. While ATMs hold considerable funds in cash, security supervision is limited to, at best, archived log and video recordings. ATMs, therefore, represent excellent opportunities for cyberattack.

In 2014 Microsoft decided to stop support for Windows XP operating system which was installed in over 95% of automated teller machine networks and cash machines worldwide. Major banks requested ongoing support from Microsoft and published plans to upgrade and replace Windows XP over time with newer operating systems or derivatives of Linux.

Yet, here in 2018, not much has changed. Windows XP, Windows 7, and Windows NT are still the most widely installed operating systems in ATMs worldwide. On a special basis, Microsoft has provided support for these Windows operating systems but that



is gradually coming to an end. Early in 2020, Microsoft will finally stop all support for Windows 7. There will be no further security updates, application patches, or technical support for ATMs that use Windows 7.

Diebold Nixdorf brought support for Windows 10 to the ATM market in early 2017 and was followed a few months later by NCR's announcement of Windows 10 support. NCR had also announced a cloud-based strategy for ATM software deployment. This new Windows 10 based technology, while required by most banks in 2020, will take considerable time to deploy.

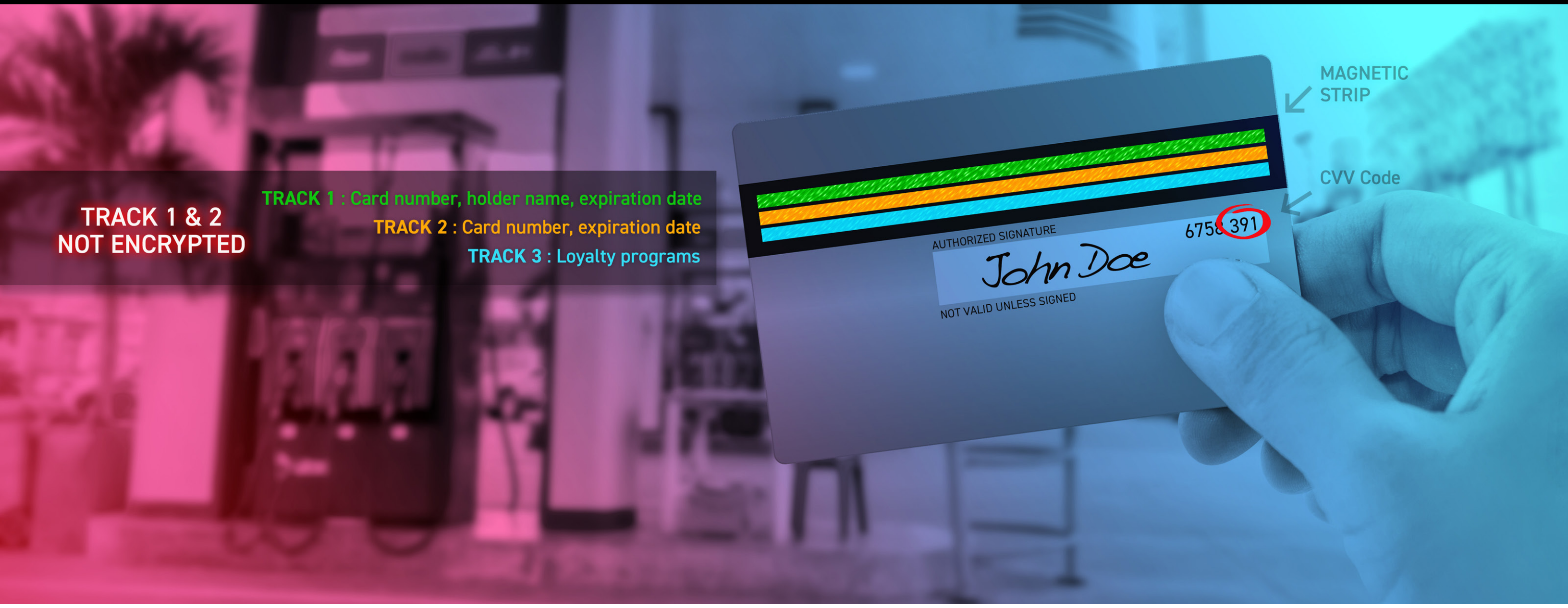
Windows 10 is not a panacea for ATM deployers. Windows 10 helps banks avert yet another crisis due to the termination of Microsoft Windows 7 support, but banks and financial institutions still have all the same challenges of keeping the ATMs updated as they would with any Windows 10 based endpoint device (workstation). Windows 7 remains the dominant operating system in ATM networks and is also perhaps the most vulnerable.

ATMs are not just simple endpoints. They are complex, high-security devices that include multiple components. Each of these components, some of which have additional embedded processors, present an additional opportunity that can be leveraged by a knowledgeable attacker.

ATM architectures generally include several standard components. This includes a card reader to read the magnetic strip on the back of the ATM card, a keypad, to process the encrypted PIN number, a speaker, a display screen, and a receipt printer. Most importantly, there is the integrated cash dispenser (safe), which manages and controls the properly authorized disbursement of cash, and tracks all of these transactions in detail. ATMs must interface with a host computer, which may be connected via a dedicated leased line or dial-up line (in the case of cash machines). The host computer then handshakes and authenticates transactions with the bank computer.

Attackers have tried to compromise ATMs directly, often by opening or physically compromising the device and then siphoning off credentials. Local attacks often compromise the card reader or pin pad or include a physical attack and penetration of the unit. More sophisticated network-based attacks, such as those by Carbanak, enable someone to compromise ATM machines thousands of miles away. These new sophisticated attacks are the most lucrative for cyberthieves and the most threatening to ATM network providers.

Attackers must be able to penetrate bank networks, perform reconnaissance to identify the ATM network components, and then move laterally to the targeted systems. Once inside, they can load additional tools and malware and then continue reconnaissance to understand the details of ATM network operation. It is just a matter of time before they can launch a successful attack.


TRACK 1 & 2
NOT ENCRYPTED
TRACK 1 : Card number, holder name, expiration date
TRACK 2 : Card number, expiration date
TRACK 3 : Loyalty programs
MAGNETIC STRIP
CVV Code
AUTHORIZED SIGNATURE
John Doe
NOT VALID UNLESS SIGNED
6758 391

Embedded Processors in Point-of-Sale Terminals

Retail point-of-sale (POS) systems are used by retail and merchant business to identify and scan merchandise intended for purchase, calculate payments, and then process credit card and/or debit card payments which link back to the bank and other financial institutions. Point of sale systems are specialized turnkey systems and have a large installed base running older operating system variants such as Windows XP and Windows 7.

Cyberattackers continue to target point-of-sale, as credit card and debit card account data continues to be in high demand on the dark web. This stolen card data can be used to order and steal merchandise before the fraudulent nature of the transaction can be detected.

New cards generally come with an EMV (Europay, Mastercard, Visa) chip and pin authentication, which can be used in "card present" transactions at retailers. Stolen card data is diverted primarily for online use, where "card not present" transactions are common, as most consumers have no chip reader with which to authenticate embedded or encrypted chip data. Stolen card data may also be used to manufacture fake cards, which in turn can be used at retailers not using chip verification. It is also believed that organized crime is doing research on the necessary procedures such that they can create a fake card with an embedded EMV chip.

Organized crime has taken a strong hand in orchestrating point-of-sale system attacks even to the point of licensing standard malware to confederates which enables them, in turn, to attack local retailers. Attackers must be able to penetrate the retailer or card processor networks, perform reconnaissance to identify the point-of-sale components, and then move laterally to the targeted systems. Once inside the network, cyberattacker tools can rapidly identify card readers and load malware that will then continually forward a stream of stolen card numbers as transactions come into the retailer operations.

Internet of Things (IoT) Devices

It is estimated that by 2020, over 25% of cyberattacks will involve IoT devices. Standard endpoint cybersecurity software does not protect IoT devices. You cannot load standard cyber defense software onto IoT devices and you do not have any visibility into what is happening inside of them.

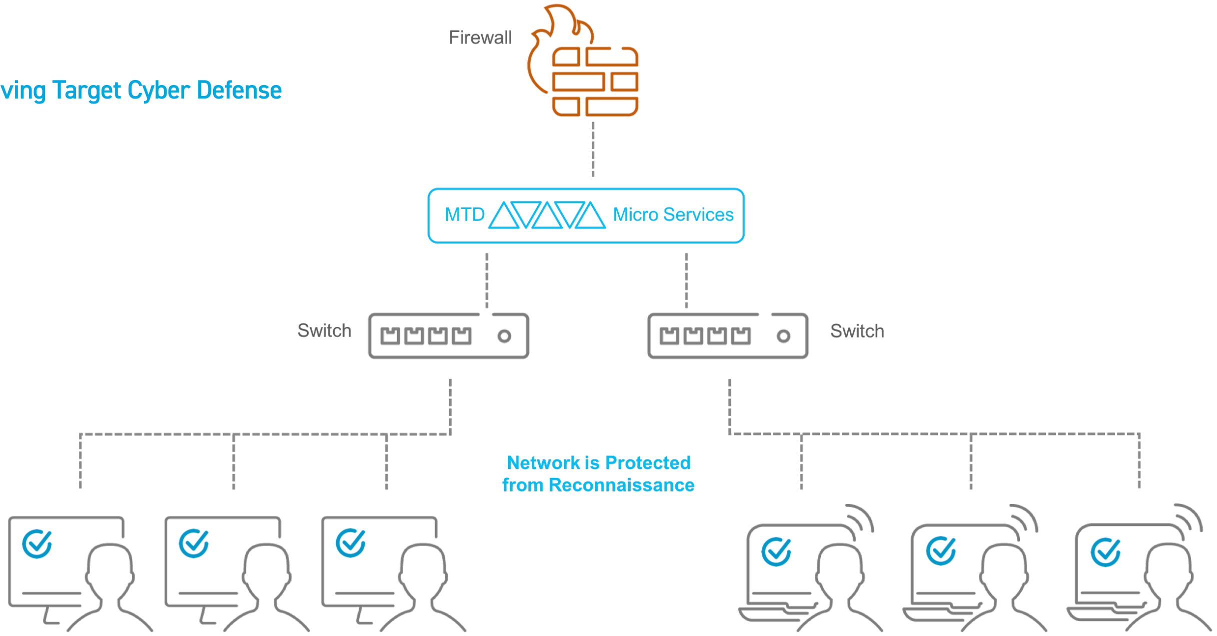
There is a broad proliferation of these devices in financial networks already. From HVAC systems to thermostats, security cameras to the large networks of security entry systems, the list is long and growing.

Many of the attacker tools that penetrate the enterprise, whether through email, memory sticks, or some other attack vector, are normally defended against by the standard endpoint protection and other security software tools. But once these malware tools propagate through the network, they can often find safe haven inside of IoT devices, where they remain undetected for sometimes months and where they provide a backdoor for extended attacker activity.

When an attacker finds an IoT device that they can exploit, they know that the enterprise cyber defense likely has neither protection for these devices, nor visibility into their operations. Of course, CISOs can attempt to restrict the use of these devices in financial networks, but all it takes is one device to allow the compromise of the entire network.

Recently we toured the RSA 2018 show and noted that solutions for protecting IoT devices were highly fragmented, very new, and overly complex. While multitudes of schemes for embedding trust and identifying and credentialing IoT devices on the network have emerged, most will take years to roll out and almost none of these solutions will help to protect the existing and growing installed base of devices within your financial networks anytime soon.

Diagram 1 - Moving Target Cyber Defense



Implementing a Zero Trust Financial Network with CryptoniteNXT

Protecting Vulnerable Devices on Financial Networks

The solution for immediately addressing all of these vulnerability use cases lies in embracing the concept and new best practice of Zero Trust. The term Zero Trust was originated by the industry analyst firm Forrester Research several years ago. It was Forrester's position that the notion of treating the internal network as trusted and the external networks as untrusted was inherently flawed. Forrester's conclusion was that every network should be considered untrusted.

Zero Trust network best practices require minimizing access to resources and visibility within the network to the absolute minimal subset you need to perform your job - no more. Traditional defense-in-depth cyber defense software and network security equipment cannot implement Zero Trust. You must combine your existing resources with new emerging technologies to build out the strongest defense to meet the needs of this running cyber war with attackers.

A Zero Trust environment constructed using MTD and network micro-segmentation technologies enable defenders to leapfrog the tactics, techniques, and procedures of the best military-grade attackers. MTD places attackers in a shapeshifting environment where IP addresses can no longer be used to map out and enumerate an attack. Classic attacker tools no longer work at all. Lateral east-west movement in the network is similarly restricted and limited by role and policy. Cyberattackers cannot target what they cannot see, and cannot attack without a target. The CryptoniteNXT platform enables you to deploy these two technologies to meet and defeat attackers, ransomware, and insider threats.

Zero Trust is Collaborative Mix of Technologies

Zero Trust draws from a wide range of technologies designed to integrate with your existing cyber ecosystem and network defenses to better secure and harden standard TCP/IP networks. New technologies such as next-generation firewalls, moving target cyber defense (MTD), micro-segmentation, deception technology, 802.1x compliant 2-factor user and device authentication, and more may be combined to enable a Zero Trust environment. Absolutely nothing should be allowed network or resource access until they have proven that they should be trusted. The goal of this empowered cyber ecosystem is to authorize, validate, manage, and enforce the identity of the system and users throughout the network.

Stopping Reconnaissance

Moving Target Cyber Defense (MTD)

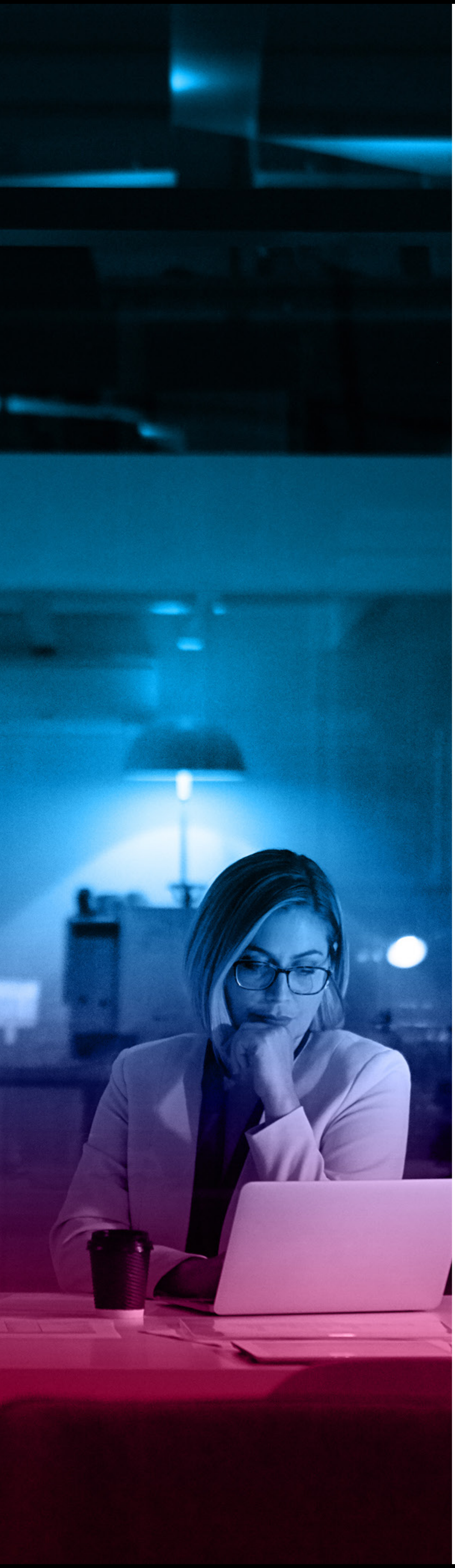
CryptoniteNXT Net Guard moving target cyber defense (MTD) deceives and contains cyberattackers at the very beginning of the attack and makes their targets invisible. Reconnaissance is completely shut down. Without visibility into the network, it is impossible for cyberattackers to map the network, access unpatched vulnerabilities, and proceed with an attack.

CryptoniteNXT Net Guard does this by transforming the endpoint's view of the network into a dynamic, abstract structure, in effect making the once static network into a dynamic moving target. Net Guard MTD creates a mapping from the obfuscated network to the real network to enable the flow of traffic across the traditional network infrastructure. Normal legitimate traffic is unaffected by Net Guard, but an attacker cannot collect actionable information about the network or masquerade as another legitimate endpoint. All of this is done without sacrificing performance or transparency to your users. CryptoniteNXT Net Guard also protects against attackers or insiders that have been resident in your network prior to installation; network mapping done prior to the installation of Net Guard is not actionable. All of this existing sensitive information is rendered useless for continued cyberattack planning.

Restricting Lateral Movement by Policy

Micro-Segmentation

CryptoniteNXT Micro Shield Segmentation significantly reduces attack surfaces accessible via lateral movement. Users only have visibility to the servers and other devices necessary to support their daily work, and attackers and malicious insiders are denied access to lateral movement beyond a very narrowly defined set of resources. CryptoniteNXT automation identifies every specific device, the approved access to resources, and the user authenticated and authorized to use it. Our automation allows you to configure and deploy CryptoniteNXT in the largest commercial and government



enterprise networks. IT staff can easily define policies within the CryptoniteNXT platform to control network access based on device types, user profiles, applications, or numerous role-based characteristics shared via Active Directory or a Lightweight Directory Access Protocol (LDAP)-based directory service. Micro Shield is also highly flexible; it supports all your existing routers, switches, and network infrastructure.

Zero Trust Mitigates Critical Vulnerabilities in Finance

Updates and Patches

The key to exploiting missing updates and security patches is to first find them. Attackers must navigate the network, move laterally, and discover and then exploit out of date software. CryptoniteNXT Net Guard does not allow reconnaissance and CryptoniteNXT Micro Shield severely restricts attacker lateral movement. Instead of being exposed to potentially dozens of vulnerabilities, the attacker is contained at the originally infected endpoint without the visibility to see unpatched vulnerabilities. The attackers cannot enumerate the network, cannot lookup vulnerabilities, and cannot identify the corresponding exploits. The risks created by overdue software updates and missing patches are thus substantially reduced.

IoT Devices

IoT devices will someday be designed with better embedded cybersecurity. That said, many millions of IoT devices have already been installed. The life cycle of this installed base is likely to be several years without replacement. A CryptoniteNXT Zero Trust environment enables you to bring in new IoT devices without worrying about the liability inherent in your installed base. If the attacker cannot find these targets, see the network, or move laterally within it, the attack is effectively over.

ATMs and POS Devices

As with our other high vulnerability environments, with Cryptonite NXT Zero Trust, embedded processors with older operating systems can no longer be discovered. They are effectively invisible. Even if an attacker has enumerated the network prior to the installation of the CryptoniteNXT platform and has obtained the specific IP of the target, that IP address will not work in a CryptoniteNXT Zero Trust environment and the device will remain safe. This is particularly useful for environments with a large number of device embedded processors in which the cost and process of replacement are prohibitively high. This includes ATM networks, point-of-sale networks, and more. With a CryptoniteNXT Zero Trust environment, all of these networks are now protected.

Key Benefits of the CryptoniteNXT Platform

The CryptoniteNXT platform provides strong benefits for the financial enterprise CISO:

- Eliminating cyberattacker reconnaissance, which shuts down the attack at the earliest possible time, reduces the time in which the attackers can breach detection, and, thus, reduces the risk of loss and damage to critical assets by a cyberattacker or an insider threat.
- Minimizing and stopping lateral movement by unauthorized parties and similarly reducing the risk of loss and damage to critical assets.
- Enabling a true Zero Trust environment, which substantially reduces the probability of a successful cyberattack from sophisticated outside attackers or malicious insiders.
- Directly addressing the highest risk use cases in banking and financial networks.
- Reducing the risk of loss and allowing the necessary delay for investment in expensive equipment upgrades.
- Reducing the risk of delays associated with the installation of critical security software patches and updates.
- Providing the same benefits of moving target cyber defense and micro-segmentation to mobile and wireless devices that access the corporate networks through partner integrations with companies such as HPE Aruba Networks.
- Stopping the propagation of specialized attacker tools such as ransomware, which extort money and threaten business operations.

Summary and Conclusions

CryptoniteNXT delivers a powerful network security solution that addresses the key vulnerabilities within banking and financial networks. By building out our Zero Trust environment, CISOs can directly address the critical vulnerability use cases that exist in most enterprise networks today. Financial application systems, SWIFT servers, online banking, credit card processing, point-of-sale systems, automated teller machine networks, and other key components of your financial network will be protected and defended.

The decision to deploy moving target cyber defense and network micro-segmentation technologies enable the SOC team defenders to aggressively defend the enterprise and defeat the most sophisticated attack techniques. Reconnaissance and lateral movement is all but shut down. MTD does not allow attackers to use their standard strategies and tools. The Cyber Kill Chain™ is broken.

Much of the new generation of cybersecurity software inside of the firewall depends on probability to ascertain a threat. Behaviors are clustered using Bayesian math, machine learning - tensorflow, or any other number of techniques. In the final analysis, machines attempt to determine that a certain group of human behavior is acceptable, and anything outside of this perimeter, or cluster, is not. Either the cluster is drawn too wide and bad actors can move unimpeded through the network, or the cluster is tight and the systems set off multiple and continual false alarms. Machine learning and other behavior-based technologies are useful, but all it takes is one successful penetration attempt to bring down your network.

Moving target defense is different - it is not probabilistic. No one within the network is trusted - at every step they must be authenticated and validated. In a Zero Trust network, when someone seeks to perform unauthorized reconnaissance or attempts to move outside of their assigned work areas, it is an immediate policy violation identified as a threat. At 100% certainty, the system automatically responds to the threat and shuts the reconnaissance and lateral movement down.

The speed of response is critical. Everything in a CryptoniteNXT Zero Trust environment is supported by immediate response and containment. As mentioned earlier, there are no alerts to resolve to action - CryptoniteNXT does that automatically. Attackers that seek to perform reconnaissance and enumerate the network are logged and alerted to the SIEM, and, most importantly, they are immediately shut down and stopped. Attacker or insider threat lateral movement out of policy is logged and alerted to the SIEM, but in a similar fashion they are restricted and shut down. If you cannot find and access internal applications, SWIFT wire transfer, automated teller machine, and point-of-sale networks, you cannot compromise them.

Find out more about how you can implement a CryptoniteNXT Zero Trust environment. Please reach out to us at sales@cryptonitenxt.com.

About Cryptonite, LLC

Cryptonite is a leader in moving target cyber defense. CryptoniteNXT enables any network to actively shield itself from cyberattacks by preventing all attacker reconnaissance and lateral movement. Patent pending moving target cyber defense and micro-segmentation technologies protect enterprise networks from advanced cyberattacker, insider threats, and ransomware. The Cryptonite customer base includes Forbes Global 2000 commercial and government customers around the world. Learn more at **www.cryptonitenxt.com.**

CRYPTONITE NXT

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.

Cryptonite, 2275 Research Blvd. Suite 750, Rockville, Maryland 20850