Barracuda®

Ransomware and Phishing

A Comprehensive Approach to Prevention and Recovery

White Paper

Executive Summary

Phishing, ransomware, and advanced persistent threats (APTs) are a serious and growing problem. The FBI estimates that ransomware alone cost businesses more than $200M in 2016—and is projected to bring in a cool billion dollars in 2017. This big money game is allowing attackers to invest significant sums to develop even more sophisticated attacks.

IT administrators and CISOs urgently need to put in place advanced, comprehensive security solutions that are engineered for the cloud era and defend against the most sophisticated new threats.

Key Takeaways

- Ransomware, phishing, and APTs are a serious and growing threat to everyone—individuals, hospitals, universities, small companies, large enterprises, nonprofits, government entities, and everyone else.
- Email-based phishing remains the number-one point of ingress for all of these threats. It begins when a user clicks on a malicious link or attachment, resulting in malware being installed on their computer.
- As users become more mobile and as workloads and data move to the cloud, it opens up a wealth of opportunities for an attack to infiltrate users' inboxes, devices, and networks. Building a security policy to counter these issues is critically important.
- The best approach to building a security policy is by using a comprehensive, layered approach capable of detecting both known and unknown (or "zero-day") threats. This policy needs to leverage real-time threat intelligence by addressing all threat vectors and all platform types as workloads migrate from physical to virtual to cloud.
- IT managers must use an email threat scanner tool to eliminate latent threats that may have evaded security measures and are currently sitting idle in email inboxes.
- As part of a multi-layered defense, IT managers must develop a comprehensive backup policy to enable recovery from a ransomware attack. This is critical to corporate data, revenue, and reputation preservation—all of which can be seriously damaged following an attack.

A New Cyber Threat Landscape

Social, economic, and technological developments cause cyber criminals to adapt by changing the tools and methods they employ, along with the systems, organizations, and data that they target.

Until recently, stored credit-card data was a prime target, since it could easily be sold in large batches on the dark web. But the market became flooded, to the point where stolen credit card data is today no longer worth the trouble and expense of stealing.

Today's online criminals have turned to extorting payments from organizations of all types and sizes using ransomware. While spyware, advanced persistent threats and other types of malware are still significant threats, ransomware has emerged as the fastest-growing tool for making big, illegal profits.

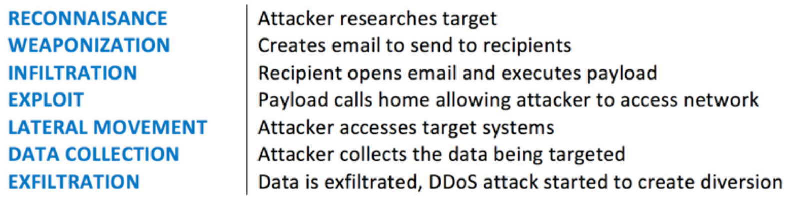
One reason for this is that it removes the challenge of monetizing stolen data—the money comes directly from the victim, with no middleman taking a cut. Another is that people share a lot of information about their lives on social media. And this makes it easy for criminals to craft a highly convincing phishing or spear-phishing email.

Manipulating users into opening a malicious attachment, or visiting a compromised URL, is in many cases easier for criminals than a technical attack against modern security.

Advanced Persistent Threats

It's quite possible that you, like many organizations, already have advanced persistent threats (APTs) residing undiscovered in your networks. Typically, these sophisticated, evasive infections are discovered only after they have been finding and exfiltrating sensitive or valuable data for months, or even longer.

The diagram below shows a typical attacker's sophisticated, multi-stage process.



RECONNAISANCE	Attacker researches target
WEAPONIZATION	Creates email to send to recipients
INFILTRATION	Recipient opens email and executes payload
EXPLOIT	Payload calls home allowing attacker to access network
LATERAL MOVEMENT	Attacker accesses target systems
DATA COLLECTION	Attacker collects the data being targeted
EXFILTRATION	Data is exfiltrated, DDoS attack started to create diversion

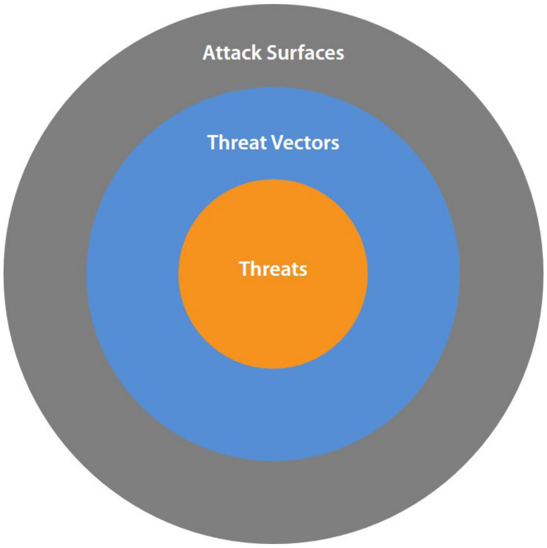
Traditional Security is Proving Inadequate

Workloads in the data center have shifted from physical to virtual to cloud as technology advancements have led to a rapid expansion in the amount of available, affordable CPU power. As you transition to the cloud, benefits include cost savings, elasticity, scalability, and simplification. The migration of data to the cloud has people posting information everywhere and retrieving it from anywhere (including ungoverned networks) and consuming it on numerous devices.

Improved mobility means data is now routinely posted and retrieved to your databases using personal devices via public, and possibly unsecured, Wi-Fi networks.
Traditional security technologies—designed to protect on-premises networks accessed through on-site desktop workstations—can't keep up with this new environment. New strategies are needed for the cloud era.

Developing an Effective Security Strategy

To protect your networks and data in this new, more complex threat environment, you need to implement a security strategy that secures against all threats, across all threat vectors and attack surfaces.



1. Threat Vectors

Threat vectors are the means by which attackers gain access to your network or infrastructure to deploy an attack. The six most common threat vectors are your network perimeter, your email traffic, passive or careless users, remote access systems, public-facing web applications, and remote users employing mobile devices.

Network Perimeter

Email

User

Remote Access

Web Applications

Remote Users / Mobile Devices

Email: This is the number one threat vector you face. Advanced security solutions have made it hard to hack well-defended networks technically. But if an attacker can craft a convincing email, and get it onto the screen of a user distracted or busy enough to just click on a link or attachment, then they've penetrated your network.

Besides training users to use caution with any email, you need an advanced email security system that can filter malicious email across hybrid and cloud-hosted email platforms. Link protection improves protection, as does the ability to detect typosquatting and other phishing strategies. Additional features that add value are email archiving, encryption, and outbound email filtering.

Network Perimeter: Network firewalls are evolving rapidly, with next-generation technology allowing extremely precise filtering and management of network traffic. Application awareness, intelligent traffic balancing, and other performance-enhancing features can increase the value of an advanced network firewall.

Users: Security would be a lot easier without users. All too often, they click without thinking, and visit sites and online apps that are inappropriate, compromised, hijacked, or downright malicious. Malware can slip in undetected while they watch a video, play a game, or check product reviews. Since you can't operate without users, the next best thing is to install a modern web gateway that enforces granular access policies, scans all web traffic to block malware (including new and unknown variants) and data exfiltration, and gives you total, real-time visibility.

Remote Users and Mobile Devices: When remote users access the internet via home or public Wi-Fi networks or other unsecured access points, their personal mobile devices may become infected or compromised. Later, when they use the same device to access your network, the infection spreads. Advanced firewall and web gateway solutions can extend policy enforcement and content filtering to off-network devices and remote users.

Remote Access: When users access your network resources remotely, there is a significant risk that attackers can harvest data in transit, leading to the ability to compromise your network. You can defend against this risk with a solution that makes it simple to establish remote VPN connections to the network on the fly, to ensure all traffic is encrypted.

Websites and Web Applications: Your business is increasingly conducted through web applications and interactive sites—outward-facing tools for interacting with customers, partners, suppliers, and others. Applications with unpatched vulnerabilities can be exploited by attackers to penetrate your network. As your online infrastructure grows more complex, an advanced web application firewall can automatically monitor and patch all your web applications to prevent exploits. It can even protect new applications and updates in development.

2. Threats

Today's sophisticated threats bear little resemblance to the simple malware—viruses and Trojans—that are scattered randomly to find targets. Those are still a danger, but now we must also contend with malware that uses multiple vectors to infiltrate parts of itself, is targeted at specific networks and individual users, and evades detection by changing its form. Advanced malware can reside in your network undetected for months, either secretly exfiltrating data or biding its time until a specific date or event triggers a ransomware detonation.

To combat this new generation of threats, you need to adopt a comprehensive approach to security. You need a solution that treats different threat vectors as facets of a unified defensive system, one that instantly shares new threat intelligence across all vector defenses. And you need a solution that can efficiently use the most advanced filtering technologies—including sandbox analysis—to block highly sophisticated threats.

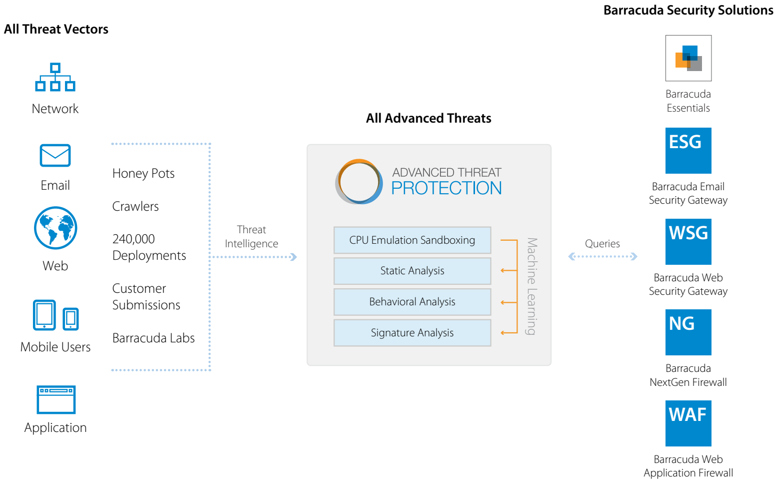
3. Attack Surfaces

As you adopt more complex, hybrid network architectures that include on-premises, virtual, and multiple public cloud deployments, old security models stop working efficiently.

Your attack surface is larger and more diverse. Without careful planning, it's easy to fall into the trap of using multiple, incompatible solutions to secure different deployments. The administrative overhead can quickly escalate out of control. And without coordinated protection across platforms, you cannot be adequately protected against ransomware and other sophisticated threats.

Effective Protection by Barracuda Networks

Barracuda gives you the tools you need to design and protect modern networks. Barracuda offers optimal connectivity between geographically dispersed locations, remote or mobile employees, and applications deployed both on and off-premises. Barracuda provides a framework for comprehensive, real-time protection to secure all network threat vectors while providing flexible deployment options to cover your growing attack surfaces. A consistent set of user interfaces and central management tools improve operational efficiencies. And Barracuda Advanced Threat Protection enables robust, highly efficient detection of sophisticated threats across all vectors.



Barracuda Advanced Threat Protection

Barracuda Advanced Threat Protection is a highly efficient and comprehensive security service that employs layered microservices in the Barracuda Cloud to sequentially filters away threats. Viruses and other signature-based threats are filtered out in the first layers. Subsequent layers detect more advanced threats so that the final layer, which uses resource-intensive sandbox detonation and analysis, only has to process a small amount of suspicious traffic.

Whenever Advanced Threat Protection discovers a previously unknown threat, it uses machine learning to add a new signature to its signature-based filtering layer. This improves security by giving every vector defense the ability to easily detect the threat. It also improves efficiency, throughput, and performance by ensuring the same malware doesn't go through sandboxing more than once—even if it attacks via multiple vectors.

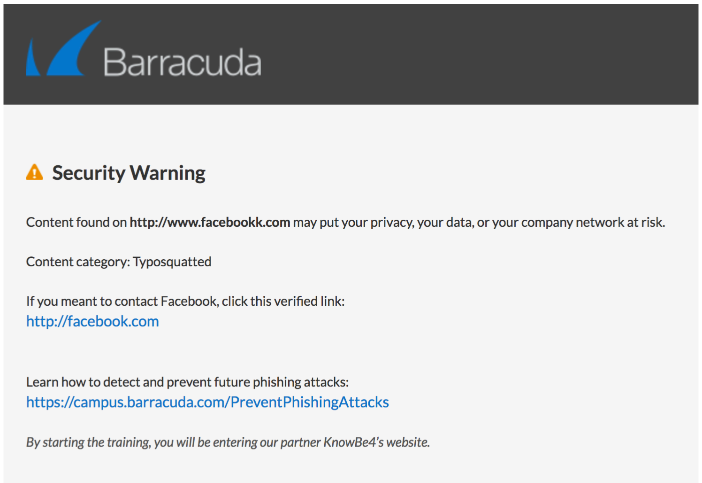
Barracuda Advanced Threat Protection is a cloud-based service available to the Barracuda security solutions that you deploy to protect your email, network, web traffic, web applications, and mobile users. It is constantly receiving and processing new threat intelligence in real time, contributed by more than 250,000 active endpoints, web crawlers, honeypots, and third-party databases, building and benefitting from one of the largest threat intelligence systems in the world.

Phishing Protection

Phishing and spear-phishing emails are designed to deceive the recipient(s) regarding their source and purpose. They may be used to entice users to enter network credentials, or financial information. They may also be used to deliver malware of any kind—including ransomware—by getting the user to click on a malicious URL or attachment.

In the case of the latest, "weaponized" versions of ransomware, a single unwise click can allow the malware into your network, after which it reproduces and spreads invisibly across networks, using a variety of traffic types.

Barracuda Essentials for Email Security effectively detects and blocks phishing and spear-phishing attempts. It combines anti-fraud intelligence, behavioral and heuristic detection, protection against sender spoofing (spammers spoofing valid email addresses), along with domain name validation. It also detects the two most common attributes of a phishing email: link protection and typosquatting.



Security Warning

Content found on **http://www.facebookk.com** may put your privacy, your data, or your company network at risk.

Content category: Typosquatted

If you meant to contact Facebook, click this verified link:
http://facebook.com

Learn how to detect and prevent future phishing attacks:
https://campus.barracuda.com/PreventPhishingAttacks

By starting the training, you will be entering our partner KnowBe4's website.

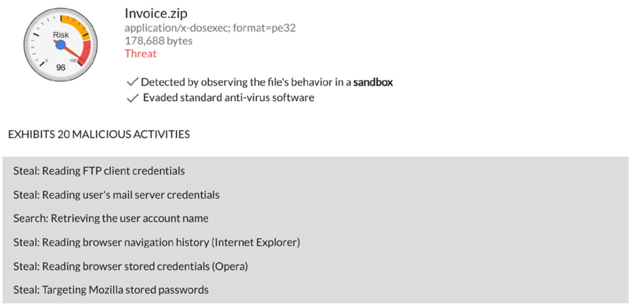
Link protection from typosquatting refers to the practice of creating malicious URLs that, at a quick glance, look like legitimate sites. The most common technique is omitting letters or using convincing "typos" that even users who check URLs before clicking often miss, for example "www.bankofarnerica.com." Barracuda Link Protection includes typosquatting detection, which automatically identifies and redirects these URLs to the Advanced Threat Protection sandbox at click time to block malicious activity.

Ransomware Protection

To neutralize the ransomware threat against your network, you need to be able to:

- **Detect** and eliminate latent threats lurking in your email boxes.
- **Prevent** new ransomware and other advanced threats from getting into your network via any vector.
- **Recover** quickly and easily from a successful attack, without paying a ransom.

Detection: Barracuda Email Threat Scanner is a unique cloud-based scanning service available at no charge. It probes your email boxes, including Office 365 mailboxes, and identifies email messages that include potentially malicious URLs or attachments, which can be used to infiltrate ransomware into your network. It also provides guidance and advice for eliminating these hidden dangers just waiting for a single unwary click.



Invoice.zip
application/x-dosexec; format=pe32
178,688 bytes
Threat

✓ Detected by observing the file's behavior in a **sandbox**
✓ Evaded standard anti-virus software

EXHIBITS 20 MALICIOUS ACTIVITIES

Steal: Reading FTP client credentials
Steal: Reading user's mail server credentials
Search: Retrieving the user account name
Steal: Reading browser navigation history (Internet Explorer)
Steal: Reading browser stored credentials (Opera)
Steal: Targeting Mozilla stored passwords

Barracuda Vulnerability Manager

According to the 2016 Verizon Data Breach Report, web applications are the most attacked and the least secured threat vector. **Barracuda Vulnerability Manager** is another no-charge cloud-hosted scanning service that scans your websites and web applications for unpatched vulnerabilities including exposure to the OWASP Top 10 (such as cross-site scripting, SQL injections, and so on). It then provides you with a comprehensive report that gives you the insight you need to repair the vulnerabilities.

Prevention: Mobile users that access data in the cloud present numerous security challenges. If a user returns to the corporate network with an infected device, Barracuda protects an infected machine from doing further damage. The **Barracuda Web Security Gateway** uses a continually updated database to identify and block access to sites known to host spyware and viruses. It also detects installed spyware trying to access the Internet. Upon discovery, it blocks the spyware activity and notifies the administrator. **Barracuda NextGen Firewalls** also detect these types of infections by monitoring and intercepting DNS traffic to known malicious sites, immediately stopping data exfiltration, and alerting the network administrator.

Recover: "Honor among thieves" is an oxymoron. When criminals use ransomware to encrypt your data, paying the ransom is a gamble. Sometimes they provide the decryption key as promised. And sometimes they don't. And sometimes, even if they do provide the key, they can always come back and re-encrypt your data again as long as their ransomware is still in your system—turning ransomware into an ongoing protection racket.

The best way to ensure rapid recovery from a ransomware attack—without paying the ransom—is to use a robust, secure backup solution that enables you to quickly and easily restore your lost data precisely as it was backed up prior to ransomware infiltrating your system.

Offsite replication of backups—whether to a separate, logically isolated second storage facility, or to the cloud—is critical to recovery. This is because certain types of advanced malware and ransomware can infiltrate your primary, on-site backup system.

To be effective, a backup solution should also be as simple and easy-to-use as possible, with automated processes and minimal resource impact. Restoring from backup should be fast, to minimize the business impacts of an attack. The solution should also, of course, be as secure as possible. Attention must be paid to securing data in transit and at rest.

Barracuda Backup is a comprehensive, cloud-integrated solution for protecting physical, virtual, and SaaS environments. Barracuda Backup is simple to deploy and easy to manage through our centralized cloud administration, and it includes built-in offsite replication. With an extensive range of supported environments, Barracuda Backup can replace piecemeal, multi–vendor backup solutions with an all-in-one backup appliance.

The Barracuda Backup Vx virtual appliances give you the flexibility to leverage your existing infrastructure. It supports replication to a remote Barracuda Backup appliance or virtual appliance, or via secure transfer to Barracuda Cloud Storage using 256-bit AES encryption.

Barracuda Backup works automatically in the background, and recovery from a recent backup file is fast and easy.

A comprehensive backup strategy is the best, last stage of protection against the damage that a successful ransomware attack can inflict—damage not only to the bottom line, but also to brand reputation, operational strategy, ongoing revenues, and executive careers.

Conclusion

Architecting a comprehensive security approach to defend against phishing, ransomware, and other email and network-born threats is a multi-dimensional challenge that IT administrators need to understand. Careful consideration should be given to:

1. **Threat vectors** – It's critical understand the different ways to effectively secure each of the primary vectors into your network:
   - Network perimeter
   - Email
   - Web applications
   - User
   - Remote access
   - Remote users/mobile devices
2. **Threats** – Staying ahead of the latest threats requires a proactive and intelligent backend infrastructure—a neural-type network that is updated in real time with the latest threat intelligence. Done right, it will operate as a highly efficient process that does not compromise security or user experience.
3. **Platform Surfaces** – Trends in work behavior have seen users move from being largely static, to mostly mobile. At the same time, technology has seen a migration of infrastructure from physical to virtual to cloud. Together, these two substantial trends require refreshed consideration as to what it means to secure both your users and infrastructure.

Because the nature of threats today is so sophisticated and complex, it is important that the appliances and applications (however they are deployed) work together to provide comprehensive security. Point products might address a specific issue, but invariably they lack the ability to give you a holistic view of a complex threat. Barracuda's products work together as a solution, giving administrators complete visibility, control, and protection against malware, spyware, phishing, spear phishing, and ransomware threats.

The Barracuda Difference

Barracuda is the vendor of choice to provide the perfect balance of value, features, and breadth of portfolio for IT professionals who wear many hats—and for organizations that contend with resource and budget constraints. Additionally, customers will also benefit from:

Common Interfaces: Barracuda's solutions share a common, intuitive interface for a familiar and consistent user experience. This makes it easy for small and medium-sized organizations to implement and manage their security solutions with minimal overhead.

Centralized Management: Our security solutions can be managed from a "single pane of glass." With our award-winning central management tools, administrators have a complete view of their security posture, from configuring policies to running reports, and much more.

Award-Winning Customer Support: Barracuda's award-winning technical support teams are always available whenever you need assistance—24/7, 365 days a year.

Threat Intelligence: All Barracuda solutions are backed by Barracuda Threat Intelligence, a powerful security framework that combines threat data collection from multiple sources around the world, advanced analysis and research, and a global operations network that supports gateway defense, endpoint security, and real-time protection through the cloud. The framework is designed to provide comprehensive, timely, up-to-date threat protection across multiple threat vectors while maintaining the highest level of performance for on-premises solutions, hosted environments, and hybrid architectures.

About Barracuda Networks, Inc.

Barracuda (NYSE: CUDA) simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications, and data regardless of where they reside. These powerful, easy-to-use, and affordable solutions are trusted by more than 150,000 organizations worldwide, and are delivered in appliance, virtual appliance, cloud, and hybrid configurations. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network security and data protection. For additional information, please visit barracuda.com.

Barracuda®

Barracuda Networks Inc.
3175 S. Winchester Boulevard
Campbell, CA 95008
United States

t: 1-408-342-5400
1-888-268-4772 (US & Canada)
e: info@barracuda.com
w: barracuda.com