Ransomware and Phishing:

How to Avoid Falling Victim to These Threats

White Paper

Executive Summary

Phishing, ransomware, and advanced persistent threats (APTs) are a serious and growing problem. The success of ransomware alone (from the perspective of attackers) is so great that the FBI estimates that it has already cost business over $209 Million in the first three-quarters of 2016—and that is just one report! This big money game is allowing attackers to increase their sophistication by plowing money back into their R&D organizations to enable even more sophisticated attacks.

Key Takeaways

- Ransomware, phishing, and APTs are a serious and growing threat to everyone – from individuals to hospitals, universities, small companies, large enterprises and so on. In short: Everyone's money is good!
- Email-based phishing remains the number one point of ingress for all of these threats. It begins with a user clicking on a link or attachment that triggers the installation of the cyber attack.
- 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 that covers all threats (both new and known). 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 address latent threats sitting in inboxes that may have evaded the above security measures by using an email threat scanner tool.
- Within the layers of 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.

Simpler Targets Have Attackers Shifting Their Focus

It's seemingly impossible today to see, hear, read or watch the news without a headline about a security breach of some sort. One thing is certain: Over time, targets and methods of attack change. There was a period where credit card theft was big news; attackers were compromising financial or commercial institutions to get access for quick monetary gain. Today, that paradigm has changed. Why? Believe it or not, the market is flooded with stolen credit card data to the point that it is now harder to sell this information. That's right—rules of supply and demand apply to the world of hacking too.

The increasing difficulty of shifting credit card information, coupled with the improved technology and procedures is causing attackers to change their focus. Unfortunately, they've moved onto something equally daunting: you.

The Internet is full of information, and social trends have people posting personal information to social media about their lives and professions, who they associate with, where they've been and so on. They do so largely without thought or consideration as to how this information could be used against them. To an attacker, this trend is the proverbial "Pandora's box" as they carefully social engineer this information into a focused campaign, waiting for the right time to strike. In fighting terms, hackers attack the soft tissues that make up your personal and professional

life and use that information to gain access to sensitive, confidential or valuable information. Knowing that it is getting harder to hack into an organization, attackers are going after easier, softer, higher value targets by leveraging attacks such as phishing, spear phishing, and ransomware.

Increasingly Sophisticated Attacks

As independent events, being phished or ransomed is pretty bad. Combine them with increasing sophistication—higher profile/higher value targets, being hit with multiple threats at once, and the right timing—and organizations face enormous challenges. While the primary method of delivery is still email, ransomware most often leverages zero-day exploits that have not been patched on your machines.

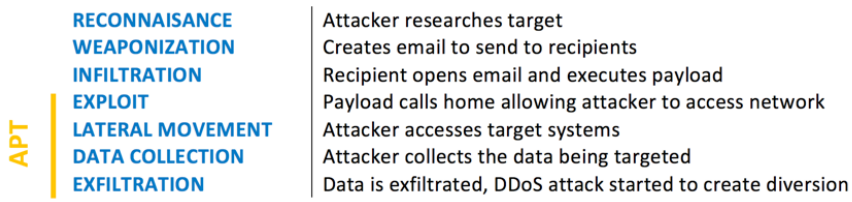
What is a zero-day exploit? A zero-day exploit is essentially a security hole within an operating system on a computer. When hackers get hold of a newly released operating system, they often scrutinize it to expose these flaws or gaps in security. Once the vulnerability is discovered, an attacker could leverage it to deploy exploits such as malware, spyware or an advanced persistent threat.

Keeping operating systems up to date is critical, and while antivirus and intrusion prevention systems are critical defenses to have in place, it might not be enough to detect an advanced persistent threat. This requires another layer of security referred to as 'Advanced Threat Detection' where a firewall or email security system will detonate any unknown or suspicious attachments/files within a sandbox environment, thereby protecting users and systems from the exploit.

Advanced Persistent Threats

While Advance Threat Detection technology prevents new unknown and known threats, it is only as good as the day the service was deployed. Infections that may have evaded existing AV and IPS systems may still be present on a server. These infections were not only architected to evade detection, but are also designed to exfiltrate sensitive/valuable data from your infrastructure over extended periods of time. These are known as advanced persistent threats.

The diagram below shows a typical process used by an attacker. From this, it is clear to see the degree of sophistication behind an advanced persistent threat (APT) attack.



Traditional Security is Proving to be Inadequate

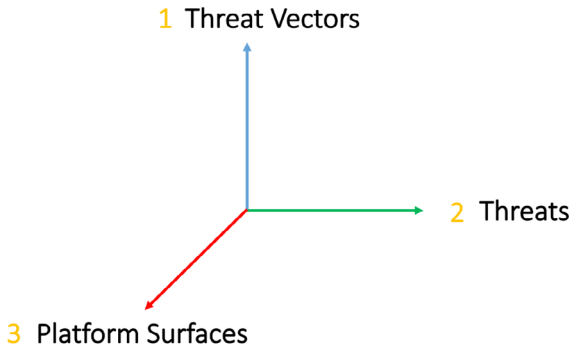
The last 10 or so years have seen seismic changes in the ways we work, communicate, and socialize in both a professional and personal capacity. Workloads in the data center have shifted from physical to virtual to cloud as CPU power dramatically increased. These days, with cloud technology becoming a viable alternative, companies are benefiting from 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. This has massive implications on an organization's security procedures and policies.

None of these things were a problem when all your users were accessing data from an on-premises data center from a desktop workstation, safely tucked away behind a firewall and other security devices. As data moves to the cloud and workers become mobile, attackers are once again looking for new opportunities to infiltrate and exploit.

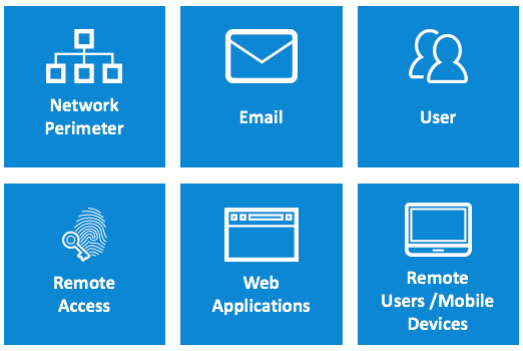
Developing an Effective Security Strategy

The issues highlighted above have created a multi-dimensional challenge that requires careful consideration:



1. Threat Vectors

Threat vectors are a path or means by which attackers can gain access to your network or infrastructure. These threat vectors are then used to deploy an attack, which itself could be malicious or could simply open a communication channel for control. While there are others, the major and most common threat vectors can be seen in the diagram below.



Network Perimeter: While most people are familiar with firewalls, there has been much evolution of the technology in this area to meet the ever-growing threat landscape and the changing platform surfaces as companies migrate to the cloud. Evolving technologies and changing user work methodologies have the network perimeter morphing constantly, and so this threat vector requires constant and careful attention.

Email: By far the most popular, if not the number one threat vector for attackers. Email lists are easy to procure, and deploying a threat is simply a numbers game for attackers. While technology takes care of most of this, users still need to be vigilant of potentially malicious links and attachments within the email.

Users: Users continue to be the one threat vector that has proven to be hardest to secure. The opportunities for introduction of threats are countless. Examples range from social engineering and social media, to use of removable media such as USB devices, mobile devices and so on. The need for increased awareness and training against threats for employees is just as critical as the most effective technology for fending off ransomware, phishing, spear phishing, and scams.

Remote Users and Mobile Devices: As mentioned earlier, user work habits are constantly evolving as new technology becomes available. 'Remote' is a broad term as users leverage home networks or public networks. Regardless, both should be considered as threat vectors since IT teams do not govern them. This, coupled with BYOD and personal devices, opens up many opportunities for a user or device to become a threat vector. For example, a personal device could be used by any family member at home, and browsing or clicking the wrong link could infect the device. When the device is placed back onto the corporate network, the threat can spread.

Remote Access: Remote access should not just be for accessing corporate resources. It is a means for workers to stay safe while they are out in the public domain. For example, if a worker operates on a WiFi service within a coffee shop, it is possible for a hacker to spoof the hotspot's SSID. The user won't know the difference—internet access will still be there. An inline keylogger could be used to procure sensitive information by the attacker. If, however, the users launched a VPN connection, all the traffic gets encrypted regardless.

Web Applications: Many, if not most, applications are now web based. Attackers often take advantage of unpatched applications or leverage zero-day exploits on servers. Another method of attack is SQL injections that can compromise data. Patching servers is often time-consuming and difficult to maintain. This is where a web application firewall comes in.

2. Evolving Threats

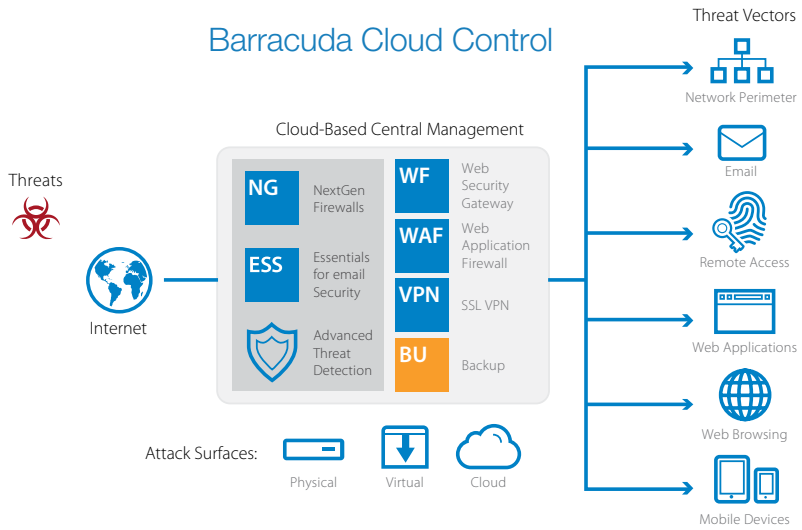
Organizations continue to struggle with providing adequate protection in an evolving threat landscape. Modern threats are difficult to detect and easily scalable. Staying ahead of the latest threats requires a proactive and intelligent backend infrastructure—a distributed, neutral-type network that is constantly updated with the latest threat data. Implemented correctly, this threat protection system should be highly efficient, capable of protecting users and data from all existing and new threats without compromising the user experience or security.

3. Changing Attack Surfaces

To complicate matters further, adoption of virtualization or public cloud infrastructures has led organizations to rethink their deployment strategies. As they look to move workloads and applications into the cloud, they are increasing their overall attack surface. Organizations must now protect their physical networks, as well as their virtual and cloud-based resources.

Effective Protection by Barracuda Networks

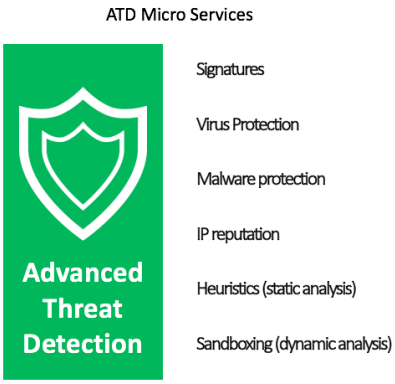
Barracuda provides administrators with the tools needed to design and a protect modern network. Barracuda offers optimal connectivity between geographically dispersed locations, remote or mobile employees, and applications deployed both on and off-premises. Barracuda provides a framework for comprehensive, real-time protection to secure all network threat vectors while providing flexible deployment options to cover your growing attack surfaces. And all of this is backed by a comprehensive and efficient threat detection system, and a consistent set of user interfaces and central management tools to improve operational efficiencies.



Barracuda Advanced Threat Detection

Barracudas NextGen Firewalls and Email Security Service benefit from Advanced Threat Detection (ATD), which is a highly efficient and comprehensive security service that consists of layered microservices that provide complete protection from all known and unknown threats.

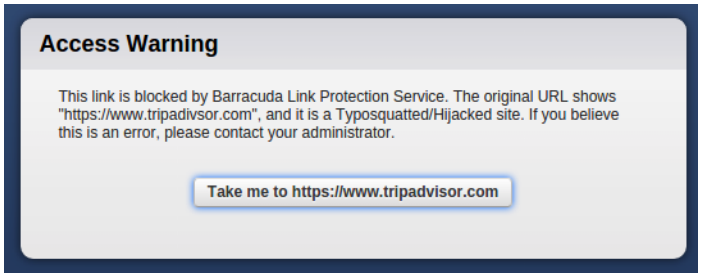
The diagram below shows how each layered microservice performs a highly specific function to filter threats from the most common and prolific, to the completely new and unknown all while maintaining an unimpaired user experience. Barracuda ATD consists of layered microservices, where each layer efficiently and sequentially filters away threats, removing the most common ones such as viruses and other signature-based threats in the first layers. Subsequent layers remove more advanced threats leaving the final layer to process new and unknown threats by detonating them in a sandbox type environment. This ensures that no matter what comes through, you are always safe—even from unknown threats.



Phishing Protection

A phishing email aims to extort sensitive information from the recipient. A highly effective call to action is used to persuade the unscrupulous recipient to click on a link that will open up a spoofed web page or seemingly credible attachment that will install malware. Barracuda Essentials for Email Security combats phishing attempts by combining anti-fraud intelligence, behavioral and heuristic detection, protection against sender spoofing (i.e., spammers spoofing valid email addresses), along with domain name validation to detect and block phishing attempts. It also protects from the two most common attributes of a phishing email: link protection and typosquatting.

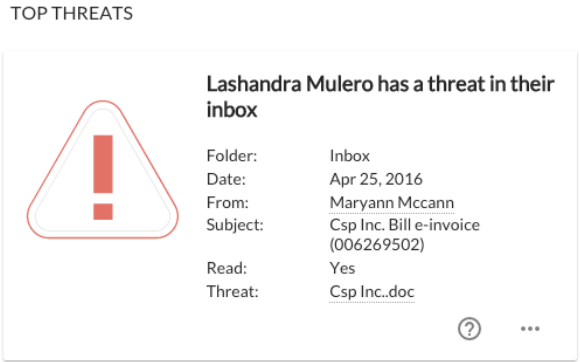
Link protection from typosquatting: More sophisticated attackers make clever modifications to URLs so they look genuine, but are not. The most common technique is omitting letters or using convincing "typos" that even users who check URLs before clicking often miss. Barracuda Link Protection includes typosquatting detection, which automatically identifies and redirects these URLs to the ATD sandbox at click time to block malicious activity.



Ransomware Protection

Understandably, many people often pay a ransom for their stolen data – largely because of time constraints, but also because the mechanisms to recover from such an attack have not been implemented. Barracuda offers customers protection again ransomware in three phases:

Detection: Advanced Threat Detection (ATD) itself is only as good as the day that the service started. Zero-day threats or infected/malicious emails that are sitting undetected in inboxes must be identified and removed. Additionally, as more businesses are migrating their email to cloud-based productivity suites such as Office 365, these latent risks and threats may already exist within the production email environment due to surpassing single layer security features. To help detect these risks, the Barracuda Email Threat Scan tool scans Office 365 mailboxes to identify latent risks that could cause problems if opened and provides remediation guidance for eliminating risks.



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: With the correct countermeasures in place, you can avoid needing to pay a ransom for the return of your data. It is important to note that if you do pay a ransom to unlock your data, it still may not remove the mechanisms the attacker put in place to steal your data. How long will it be before the attacker decides to switch it back on and ask for a further ransom payment? Perhaps it's only a matter of time before ransomware turns into "Protectionware." This risk is why having a backup solution is a key defense layer against ransomware. Specifically, the IT manager must develop and employ a solution that addresses 'Recovery Point Objectives' (RPO). Instituting a restore to the appropriate point in time will ensure that only the data between backups is all that is lost.

Barracuda believes that data protection should be simple, easy, fast and cost-effective. Barracuda Backup is a comprehensive cloud-integrated solution for protecting physical, virtual, and SaaS environments. Barracuda Backup is simple to deploy, easy to manage through our centralized cloud administration and offers built-in offsite replication. With an extensive range of supported environments, Barracuda Backup can replace multi–vendor piecemeal backup solutions with an all-in-one backup appliance, while the Barracuda Backup Vx virtual appliances provide organizations the flexibility to leverage their existing infrastructure. Barracuda Backup supports replication to a remote Barracuda Backup appliance, virtual appliance, or secure transfer to Barracuda Cloud Storage using 256-bit AES encryption.

Again, putting together a comprehensive backup strategy will ensure that the only thing your company will lose is the data between backups, which is a much lower price to pay than a ransom, your company's reputation, lost revenues, or possibly even jobs.

Conclusion

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

1. **Threat vectors** – Although there are others, there are six main threat vectors that need to be secured:

- Network perimeter
- Email infrastructure
- Web applications
- Web browsing
- Remote access
- Mobile devices

2. **Evolving Threats** – Staying ahead of the latest threat 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. **Changing Deployment 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 move 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 complex with ever increasing sophistication, 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

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 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, end-point 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 both on-premises solutions and hosted environments.

About Barracuda Networks, Inc.

Barracuda provides cloud-connected security and storage solutions that simplify IT. 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 deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.

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