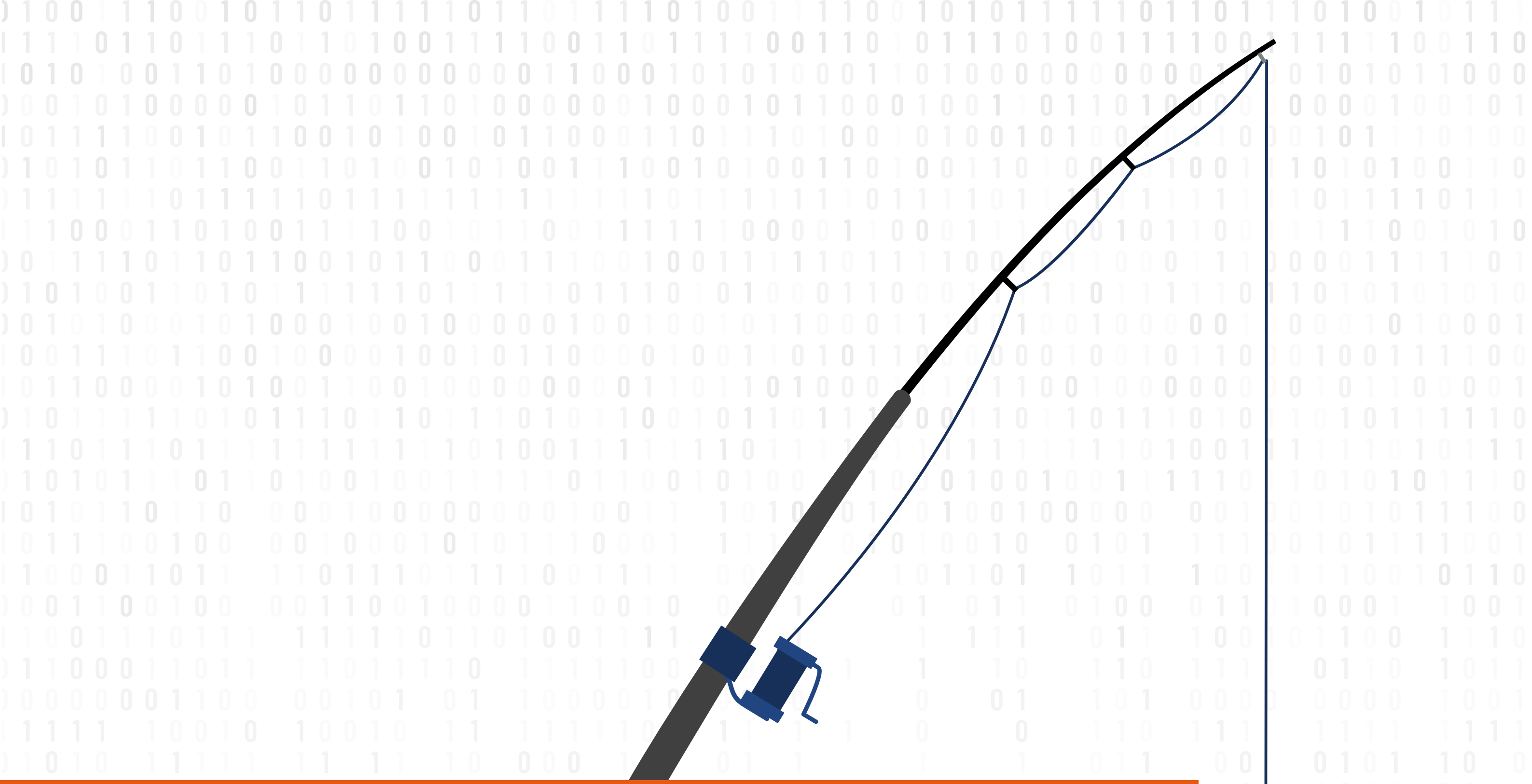
ALTIMETRIK®

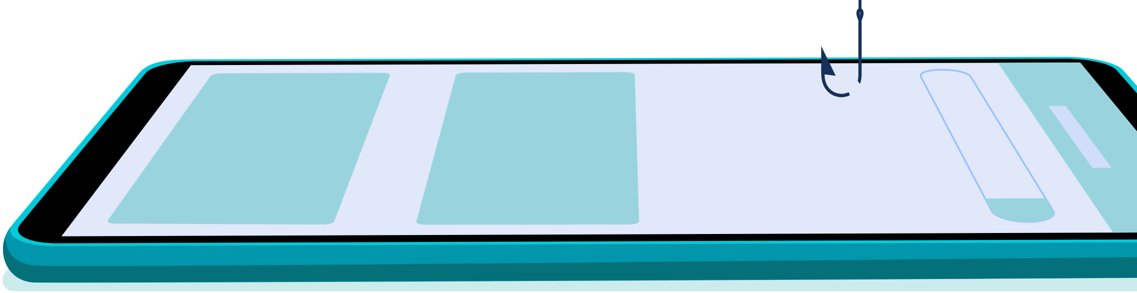
DEEP-SEA PHISHING

BulletProofLink Phishing-as-a-Service (PhaaS)



Microsoft and its products are one of the top targets of cybercriminals across the globe. While investigating phishing attacks, Microsoft recently reported developments, uncovering a large-scale PhaaS operation called BulletProofLink. The service (aka Anthrax) offers a robust set of services for cybercriminals, including customer hosting and support, the sale of phishing kits, phishing email templates, and automated services with attractive price points. After careful analysis during the investigation, Microsoft ensures that Microsoft Defender for Office 365 protects its customers from the campaigns that BulletProofLink enables.

Companies should not let their guard down; Phishing is big business and is evolving. There will be more attempts on Microsoft and others because of the particularly attractive nature of PhaaS and other phishing kits. Cybercriminal groups can leverage these services in either a subscription-based model or a SaaS model, which includes hosting, phishing emails, and credential theft. It's an out-of-the-box solution that is irresistible to fraudsters and cybercriminals.



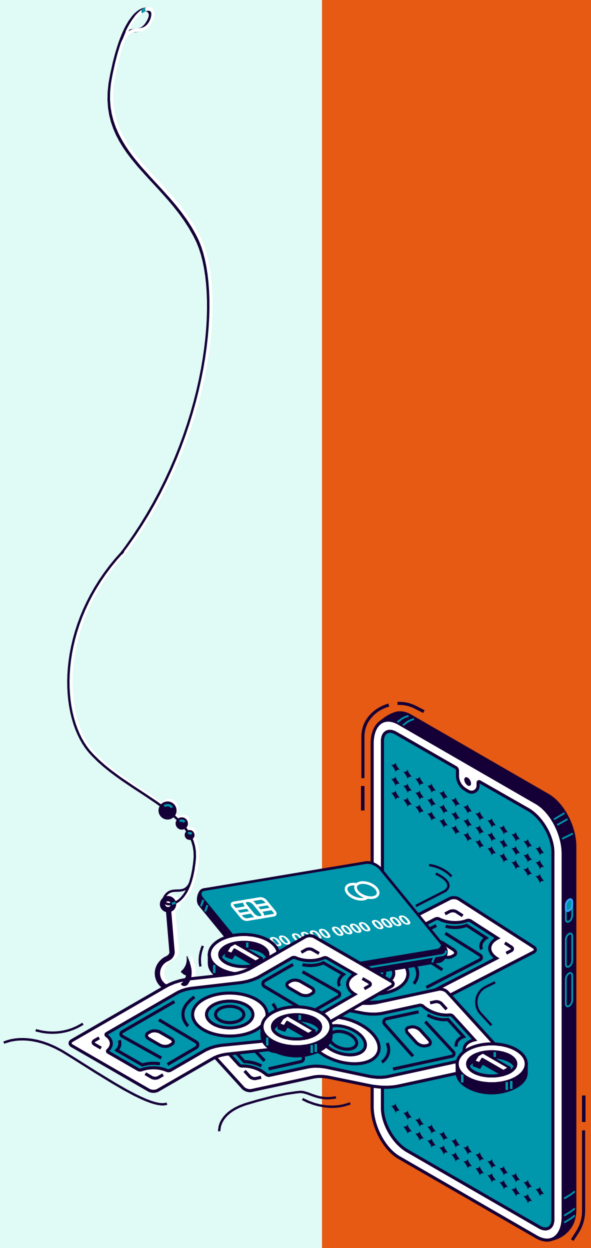
Phishing and PhaaS kits include:

- End-to-end tools needed by a cybercriminal for their trade
- Email templates designed to evade detection
- Portals that offer domain names and websites that are customizable for phishing purposes
- Subscription services for the deployment of phishing campaigns, false page sign-in development, hosting, credential theft, and redistribution

A Brief History of Cybercrime Hosting Services

Cybercrime hosting services like MoreneHost are well known in the underground, having provided similar services dating back to 2009. Offerings services included everything from data exfiltration to phishing sites, credential dump shops, and malware command control infrastructure. Operators have hosted these cybercriminal services on IPs located in Moldova and the Netherlands in addition to hosting the infamous banking trojan Zeus or Panda Banker [1] [2].

Zeus is a Trojan horse used to steal banking credentials by keystroke logging and form grabbing. Zeus is spread by drive-by downloads and phishing. Discovered in 2007, it became widespread in 2009 where it was later discovered that Zeus had compromised over 100,000 computers and accounts on websites of companies with .com and .org domains like the Bank of America, NASA, Monster.com, ABC, Oracle, Play.com, Cisco, Amazon, and BusinessWeek.



BulletProof hosting has been around for some time, however, the "industry" has evolved. The advent of even more advanced services like BulletProofLink - has expanded the accessibility to lower-skilled attackers with a point-and-click attack framework at a lower investment of time and cost. Curious young inexperienced hackers, "script kiddies", are approached by seasoned hackers who provide them with the tools to do low-level surveillance and attacks. These script kiddies are a ripe network that becomes the first line of infiltration by seasoned hackers and they [3] [4] provide access to advanced tool frameworks and attacks that were before unheard of 10 years ago. To access an online portal, pay a subscription fee or pay for the service and you're ready to launch sophisticated attacks with supporting newsletters, tutorials, and training videos.

The scale of the service operations and accessibility have proliferated. Distributed phishing campaigns, where attackers launch campaigns with ease to steal credentials. They've created a service that's easy to use, distributed it to a wider audience of users, and earned millions for providing access to the platform. The service operators reap benefits from users of the platform and create what is known as "double theft.". They're stealing credentials from their cybercriminal clients as well.

Companies must deploy the latest anti-phishing techniques. The broader community benefits from these advancements and uses them to enhance email filtering rules in addition to threat detection technologies like sandboxes for threat simulations.

The security community needs to work together and collaborate with greater frequency to turn the tide on cybercrime. Security is everyone's responsibility across an organization. Gone are the days where the sole responsibility of security lies with the Information Security department. It's now vital imperative for all functional groups to learn how to secure their information and technology. Cybersecurity training should not be an activity that is done once during the onboarding process however should promote sharing the latest developments in knowledge with periodic mandatory security training.

What is the cost of a breach?

The scale of coordinating phishing operations is growing and unfortunately, we are the target, especially since business email compromise is a hot commodity. It is estimated that in 2019 there was a worldwide loss of $17,700 per minute due to phishing attacks. IBM's Cost of a Data Breach Report found that on average a compromised record cost approximately $150. Using that as a metric we can deduct the cost of a specific breach based on the number of records stolen. FBI reported that business email compromise (BEC) reached an incredible $1.8 billion in 2020, demonstrating how lucrative an operation this is for cybercriminals.

Understanding the breadth of impact in how these costs are calculated provides a clearer picture of how disruptive a breach is. First, there is the loss of work hours plus employees' equipment is subject to incident response and remediation efforts. Then there's the damage to the brand reputation of the business, and in some instances, a company may lose intellectual property in addition to the revenue it generates. On top of these losses, the firm may face significant compliance fines, legal fees, regulatory scrutiny, and ongoing audits. Security and preventive measures are expensive; however, more organizations recognize that not investing in them may lead to the company facing further damage to their brand while risking the loyalty of their customers. That is a far greater risk to their business and bottom line.

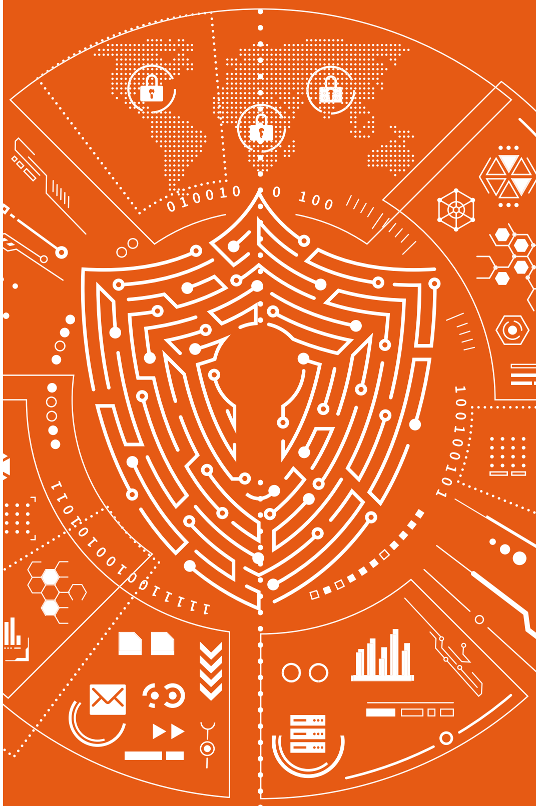
How Altimetrik defends against phishing attacks

Preventing phishing attacks starts with educating employees on how to identify them. This includes conducting training sessions with mock phishing scenarios and updating staff on the evolving nature of phishing attacks. It is also important to educate and test executives within the company, as they are prime targets. Many companies will send phishing emails to their employees, and those that "fall for them" are required to take a refresher course to reinforce how to avoid being scammed.

Proactive organizations will know which steps are necessary for raising awareness, including arming their employees with the skills necessary for recognizing and dismissing phishing attacks. Employees must also learn this includes any request they see for sensitive information or asking the user to click on a suspicious link, should raise a red flag and be reported to the security or helpdesk team. Many companies have also made their customers aware of the risks associated with phishing campaigns and suggest that all requests for personal information should be viewed with suspicion. Companies also stress that customers have alternative methods for requesting, sharing, and obtaining information. Consider who sent you the email. Is this a known trusted sender or brand impersonation?

Employees should keep an eye on any website content and URLs they are invited to click on, as attackers leverage slight typo-jacking, or a slight misspelling of an email or website address, to mislead customers into using their malicious sites. Many phishing attacks will send an email using a senior executive's name while in reality it was sent by a cybercriminal. Clicking on the sender's email address will confirm who the sender is, as well as inspect headers and URLs by hovering over them to reveal the true source and destination of the request.

IT teams must take preventive action that enables proactive, consistent, and scalable policies with practices to keep phishing at bay and stay ahead of attackers. Deploying security products, services, spam and web filters, secure email gateway and post-delivery protection can increase an organization's chances of avoiding an attack.



Other basic steps include:

- Convert HTML in email messages or disable script, with appropriate prompts wording to open or download images from a trusted source.
- Analyze your emails, attachments, and URLs.
- Block known bad actors, leveraging shared resources from leading security companies.
- Configure email servers to prevent spoofing and replay attacks.
- Ensure that devices like laptops and mobile phones are up to date with current security patches and that ensures all devices have been backed up.
- Prevent employees from downloading software without authorization.

It will also be necessary for organizations to make investments when it comes to remote access and identity management solutions, which may also need fundamental changes to the way they currently operate. IT leaders must take steps to:

- Deploy multi-factor authentication to protect your accounts, which makes it harder for attackers to log into accounts even if they have been compromised.
- Deploy malware and antivirus solutions, ensuring signatures are up to date and monitoring equipment .
- Require VPN for all remote employees.
- Encrypt all your sensitive information to ensure you have appropriate data classification and policies in place.
- Deploy security policies that include password durations, password expiration, and complexity.

Cybercrime and phishing are now becoming commonplace. Organizations understand the dangers and many companies have taken steps to protect their assets and customers. Cybercriminals have built an efficient, far-reaching infrastructure and network to launch sophisticated attacks on a regular basis. Unfortunately, phishing has become a mature and lucrative business due to the aggressive and innovative nature of cybercriminals looking for new ways to scam others. Education can only go so far if it is not reinforced. Each of us must be diligent and understand what techniques are used by scammers and ways to avoid them. As the world becomes more sophisticated and connected by a proliferation of devices, the risks of phishing and other cyber threats will also increase. Security has always been and will continue to be an arms race with real consequences.

ALTIMETRIK™