Here are 7 important takeaways from the 2018 Ponemon Institute's "State of Endpoint Security Risk" Report:

1. **Endpoint-focused attacks are increasing.**
   Over 60% of respondents in the 2018 State of Endpoint Security Risk survey indicated that over the past 12 months, the frequency of attacks has increased. An increase in successful endpoint security attacks is concerning, because this means organizations must be better prepared to prevent endpoint attacks and organizations must also be prepared to respond to the threats that are evading their cybersecurity defenses.What's more, according to respondents, an average of 52% of all attacks cannot be realistically stopped. If preventing attacks isn't possible, mitigating the damage of a data breach is—if you're proactively hunting for attacks already in progress.
2. **The average cost of a data breach has increased from $5 million to $7.1 million.**
   Recovery costs, notification costs, and losses to IT infrastructure, productivity, and data/information has increased by over 40%. This $7.1 million data breach costs, factors out to an average of $440 per impacted endpoint. If we look specifically at SMBs and mid-sized companies, the average cost per impacted endpoint increases to $763.
3. **Over 60% of survey respondents claim their organizations were compromised in 2018.**
   In fact, 64% of respondents claim their organizations were successfully attacked this year—up from 54% in the 2017 endpoint security survey.
4. **Zero-day attacks—or attacks via an unknown application exploit or software vulnerability—are 4x more likely to be the culprit.**
   Just over 75% of the respondents who claim their organizations were compromised in 2018, attribute the attack to unknown zero-day attacks and/or new threats. By contrast, only 19% of respondents claimed their organizations were compromised by a known, or existing, attack.
5. **Antivirus tools missed an average of 57% of attacks.**
   As malware, attack types, and attackers evolve, we're seeing that AV (even "next-gen" antivirus) software are missing the majority of attacks. Based on respondent estimates, only 43% of attacks are blocked by antivirus tools/software. Endpoint security survey respondents blamed a high rate of false positives and alert fatigue as the issues preventing them from getting the most out of their antivirus software.In other words, antivirus may be flagging too much and too many attacks, while inadequately protecting your company from unknown threats and malware.
6. **Organizations are vulnerable. In fact, it takes 102 days (on average) to patch/repair endpoints.**
   It's difficult to keep endpoints and systems operational through effective patching—for organizations of all sizes. Over 40% of survey respondents have employed a process to deploy and manage patches to their endpoints, but these patches take longer to roll out, due to concerns with the impact on business continuity and system performance. Vulnerabilities can exist within applications, operating systems, and firmware, so it's important to take proactive steps to continuously scan your network and nodes for vulnerabilities using a tool like Infocyte HUNT.
7. **Organizations are frustrated by the lack of adequate protection and implementation challenges offered with EDR tools.**
   EDR, or Endpoint Detection and Response tools, are designed to detect and "block" the early signs of an attack. Unfortunately, with the rise in zero-day exploits and new/advanced malware, organizations are finding that EDR and preventative technologies are not as effective as they thought.Moreover, 47% of respondents that have EDR tools deployed within their organization needed over 90 days to implement. Plus, less than half of the functionality of EDR tools (46%) are actively employed and used.

In conclusion, your endpoint security infrastructure should include defensive technologies, but preventative cybersecurity tools alone are not enough.

It’s just as important to employ proactive or “offensive” cybersecurity tools and techniques, such as threat hunting and regular compromise assessments, to ensure your organization is better protected from advanced malware and malicious threats.

7 Stats That Show Why Cyber Threat Intelligence is a Must for 2019

by Nathan Teplow / November 28, 2018

There’s a lot of talk these days about Cyber Threat Intelligence (CTI) because it gives organizations an opportunity to be proactive, rather than reactive, in their cyber defense. There are many interesting use cases for CTI, but it takes an investment in tools and people to be used effectively. So how do you know it’s worth the investment and is it something your organization should consider in 2019?

Let’s take a look at 7 statistics that demonstrate how CTI can help your organization defend proactively and reduce your overall cyber risk.

#1: There’s Been a 297% Rise in Retail Phishing Websites over the Last Year

In our Retail Threat Landscape Report, we observed a 297% increase in retail phishing websites. Why is this important? Threat actors like to target the weakest link, which more often than not is your customers. As organizations continue to bolster cyber defenses, cybercriminals are attempting to circumvent those defenses by targeting consumers directly. In addition, new tools, like Phishing Kits, have lowered the hacker “barrier-to-entry”, meaning less sophisticated hackers are able to run their own campaigns, and do so at a faster rate.

Further Reading: Find out how Hacking-as-a-Service is changing the threat landscape

This has made it increasingly challenging for organizations to protect customers and brand reputation from this increase in consumer phishing activity. Using cyber threat intelligence to monitor for new phishing domains can help you extend phishing protection to your customers by taking down domains before before they’re ever used in an attack.

#2: 71% of Organizations Who Do Not Deploy a Threat Intelligence Solution Say it is Difficult to Prioritize Threat Intelligence Data

This was a key finding from a Ponemon Institute study on the value of threat intelligence. Cybersecurity teams have a lot of incidents to investigate and respond to, so any help identifying critical issues and prioritizing work is helpful. Comparing threat data to your digital assets can help you add context and relevance to your intelligence, enabling you to prioritize workloads and understand if and how a threat impacts your organization.

#3: Over 23% of DevOps Servers are Openly Accessible via the Web

Cloud-based SaaS solutions are great for productivity. Different departments can now implement technology solutions on their own, without the need of IT or the security team's involvement. However, these departments often misconfigure access and sharing permissions, leaving data and sensitive materials publicly exposed, if you just know where to look.

In our research report, DevOps Beware: Your Servers Are Open for Business, we found that over 23% of DevOps servers are openly accessible via the web, either fully exposed or behind a simple login page (which be guessed or brute-forced for access). Cyber threat intelligence can help you monitor for misconfigured servers and databases, so you can lock down any accidentally exposed data before an unauthorized party accesses it.

#4: 149% Increase in Credit Card Details for Sale on the Dark Web

Credit card fraud is nothing new, but the internet has enabled increased access and opportunities for making fraudulent purchases. In our Financial Services Threat Landscape Report, we observed a 149% increase in credit card details for sale on the dark web. Monitoring the dark web for your BINs and key account numbers can help you identify when your details have been leaked and lock down accounts before any fraud is committed, which can save organizations millions of dollars each year.

#5: 56% of Organizations Experienced a 3rd Party Data Breach in 2017

This stat comes from a study done by the Ponemon Institute, titled Data Risk in the Third-Party Ecosystem. Vendors, partners, suppliers, integrators, acquisitions and any other organization that holds/shares a company's data all contribute to overall cyber risk. Companies must regularly assess and manage risk for their cyber supply chain, and can do so by extending cyber threat intelligence to cover their 3rd party organizations.

#6: 40% Increase in Corporate Credential Leakage

This is another finding from our Financial Services Threat Landscape Report. Leaked credentials are one of the simplest ways for unauthorized parties to gain access to corporate systems, and there's no limit to leaked login credentials you can find on the dark web. Monitoring forums, paste sites and other underground data exchange forums can help you identify leaked company credentials in real time so you can lock down or reset those credentials. Leveraging automation and directory integrations can help you speed up the mitigation process, so you are closing holes quickly before any damage is done.

#7: Expected 3.5 Million Unfilled Cybersecurity Positions by 2021

It’s no secret that there is a shortage of cybersecurity talent across the world, but it is important to consider as you plan to evolve your cybersecurity defenses and programs. Organizations need help working smarter, not harder, and cyber threat intelligence can help you look beyond your firewall to anticipate cyber threats.

Protecting your Brand and Executives in an Increasingly Digital World

by Kyle Montibello / December 6, 2018

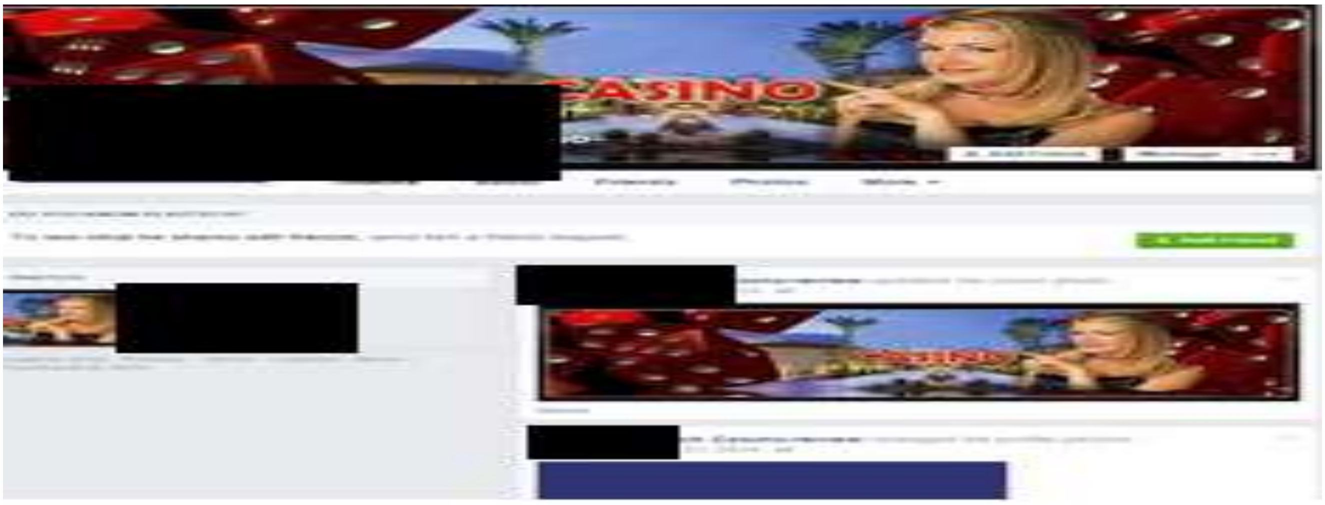
You know how important your brand is. It’s an identity, a reputation, an expectation, and a promise to customers. You know the importance of protecting that brand, but can you spot others trying to impersonate your CEO on Twitter or identify fake apps that mimic your company and/or brands to steal customer information? As companies have extended their brand into the digital world, they open up new attack vectors and face new risks they must defend against.

Here are some of the key cyber risks that organizations must consider in order to protect their brand and executives in today’s digital world.

What is Brand Protection?

Most people understand what brand protection is at a high-level, but what do we mean when refer to protecting your brand in a digital world?

Brand security issues typically take place outside of your traditional security tools, like your firewall, IDS or endpoint protection. Instead of protecting a network, you are protecting a concept, the image that is your brand. There are lots of tactics that can harm your brand online. A common one is fake social media pages.



[redacted]

[redacted]

[redacted]

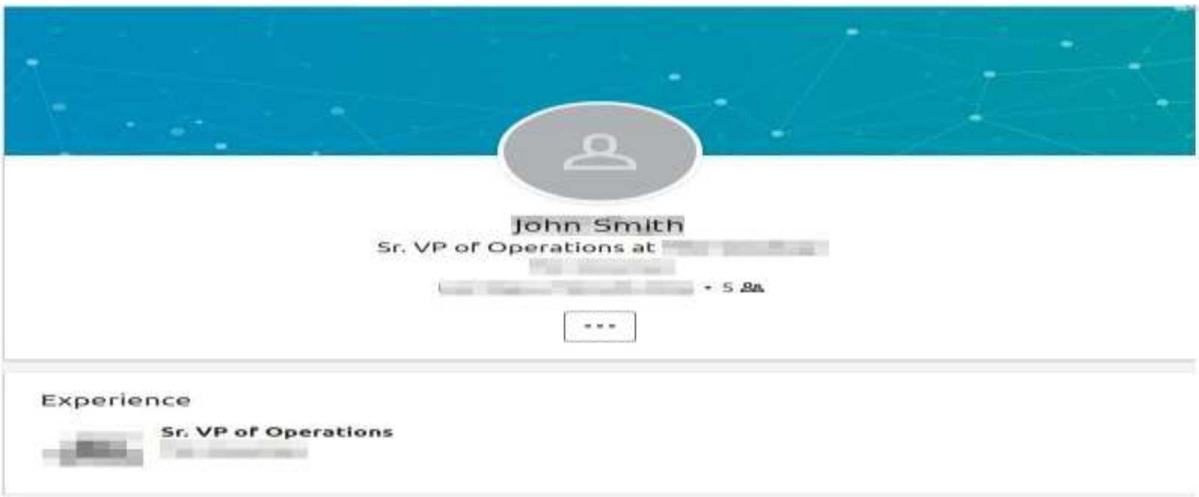
[redacted]

Many organizations have invested in building their social media following, but they haven’t considered the cyber risks that come with that. It is easy for anyone, whether it be a simple internet troll or malicious actor, to make a new Facebook (or any social media site, for that matter) page using your company name and logo, then use this fake profile to interact with your customers.

Even though this tactic is “out of your control”, it can be incredibly damaging to your brand, especially if one of your customers is duped. Without a process or tool that monitors social media for fake accounts, it’s very difficult for organizations to take protect against this vector.

The importance of external digital protection goes beyond the company, it is also applies to protecting your people.

Executives & VIPs



John Smith

Sr. VP of Operations at

• 5

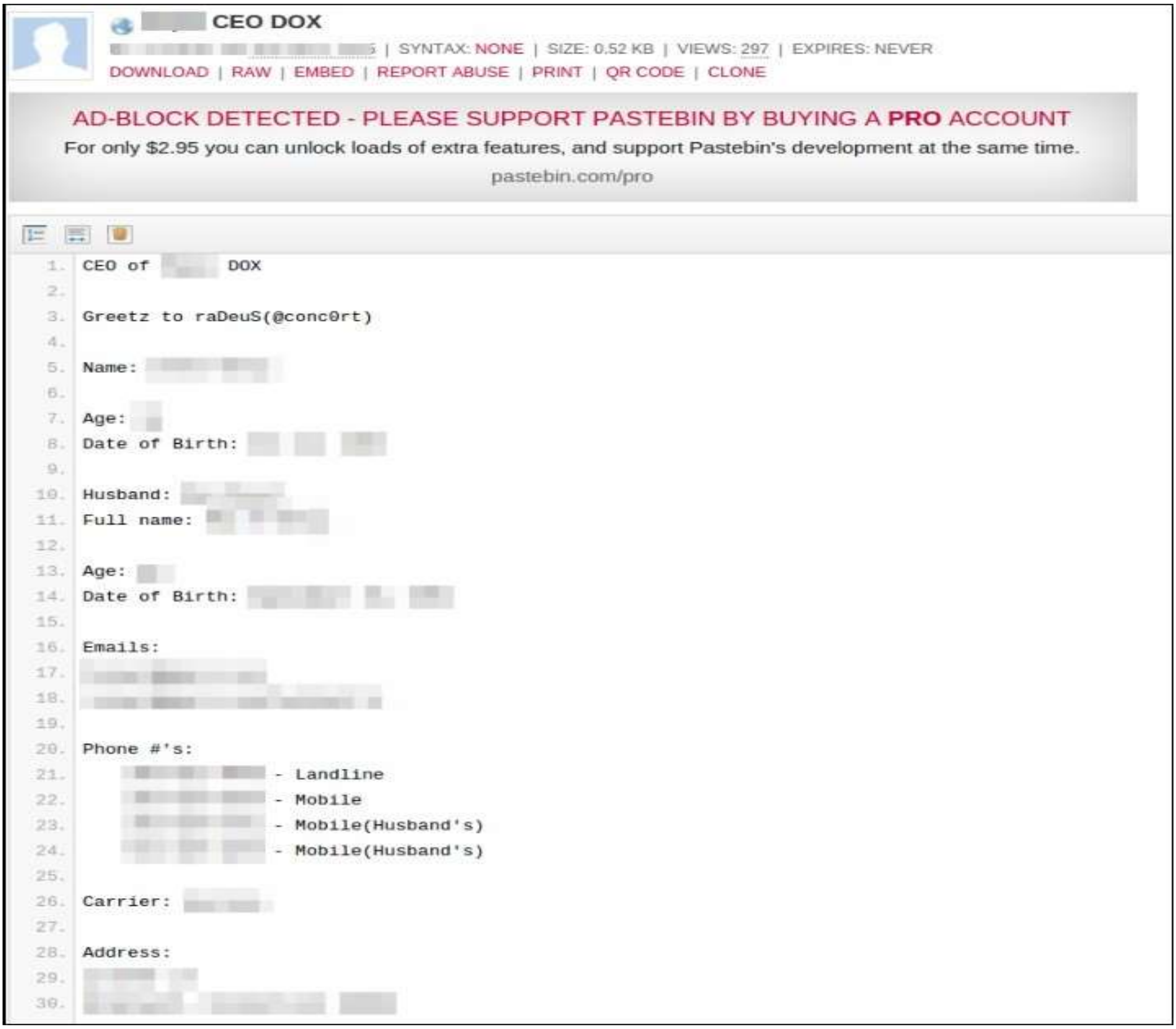
Experience

Sr. VP of Operations

Beyond company profiles, pages impersonating executives or key employees can be made just as easily. We find countless pages impersonating key employees, which is a tactic often used in targeted phishing and social engineering attacks.

Digital executive risk goes well beyond social media into the dark web. Sensitive data is constantly posted on hidden forums or sold on black markets, which poses a risk to all your employees, but to executives in particular. Targeting high-value or high-wealth individuals provides cybercriminals with more opportunity to run schemes and make money, so protecting their PII online is critical.

The next example shows a post containing personal details of a CEO and family that were leaked on the dark web. A leak like this is a huge breach of privacy and creates a physical security concern by making phone numbers and addresses available.



[redacted] CEO DOX

[redacted] | SYNTAX: NONE | SIZE: 0.52 KB | VIEWS: 297 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT | QR CODE | CLONE

```
CEO of [redacted] DOX

Greetz to raDeuS(@conc0rt)

Name: [redacted]

Age: [redacted]
Date of Birth: [redacted]

Husband: [redacted]
Full name: [redacted]

Age: [redacted]
Date of Birth: [redacted]

Emails:
[redacted]

Phone #'s:
       [redacted] - Landline
       [redacted] - Mobile
       [redacted] - Mobile(Husband's)
       [redacted] - Mobile(Husband's)

Carrier: [redacted]

Address:
[redacted]
```

Customers

A phishing attack that targets customers and harvests their payment and/or personal details with a fake shopping page isn't just lost sales, it is comparable to a security breach exposing customer PII. Even though this attack is completely outside your domain or systems, if a customer is phished from a campaign using your brand, they're likely going to blame you. Another common customer phishing vector is application stores. Add sentence or two about this vector and how its used...

Protecting your brand is protecting your customers. When a brand gets attacked, it is often loyal customers who are targeted. Monitoring for and shutting down potential attacks before your customers become victims is key to protecting your brand online.

Brand Misuse

Another threat you must protect against is brand misuse or false association. This often occurs when a company or individual wants to boost themselves by piggybacking on your reputation. It is very common to see this in eCommerce, where third-party stores will claim to be an authorized retail partner, yet have no official association with your organization. Monitoring for misuse protects customers from fake sites and strengthens your partnership value for the resellers and partners you work with.

About IntSights Brand and VIP Protection

Our platform's tailored threat intelligence enables organizations to continuously monitor for and identify potential cyber threats to your brand and/or executives. Using key assets that map to your digital footprint (brand names, social media pages, mobile apps, executive & VIP names etc.), we identify specific threats, including a screenshot, to brand impersonation and create a ticket with that information for your security team to review. Perhaps most importantly, we also enable you to take down brand and executive threats through our partnerships with social media sites, registrars and application stores, so these threats can be mitigated quickly and efficiently.

15 Technologies and Tools Commonly Used in Dark Web Black Markets

by Itay Kozuch / July 3, 2018

When it comes to dark web black markets, anonymity is key. To help maintain their anonymity, dark web black market users leverage a variety of tools and technologies that mask their identity and location. It's important to know how these tools are used so you can perform reconnaissance and identify potential attacks or leaked information that can be used against you. Here is our list of 15 common technologies and tools used by cybercriminals to access and communicate via the dark web.

In addition, don't forget to check out our 10 Dark Web Black Market Terms Every Cybersecurity Professional Should Know.

Dark Web Black Market Technologies & Tools

1. **Cold Storage:** A secure offline wallet for your Bitcoins or other cryptocurrencies.
2. **Cryptocurrencies**: By now, you're likely familiar with cryptocurrencies. Naturally, they're a very popular method throughout dark web black markets. Here are some of the most popular cryptocurrencies used across black markets:
    1. **Bitcoin:** An open source, peer-to-peer payment network and anonymous digital currency being used for almost all transactions on the darknet.
    2. **Litecoin:** An alternative cryptocurrency, similar to Bitcoin. The key difference is that while Bitcoin uses hashcash-SHA256^2 as the 'proof of work', Litecoin uses hashcash-Scrypt, which is designed to use more memory and be less subject to custom hardware designed to solve the problem quickly.
    3. **Monero:** A newer, more privacy-focused cryptocurrency that's being accepted by some Dark Web black markets.
3. **Emergency BTC Address:** An address to be held on record to send all funds to in case of a market shut down. This would ideally be a cold storage address with no information that could be used to connect the owner to their identity. This address would only be checked after a market was shut down in order to recover outstanding funds.
4. **Grams:** Cross Marketplace search engine for the Dark Web.
5. **Hidden Service:** A term for a .onion domain name. It can only be accessed through the Tor network, and cannot be seized by a government or law enforcement agency.
6. **Hushmail:** An email provider used by many Dark Web users that focuses on privacy and uses industry standard protocols PGP and 256-bit AES encryption. It claims to be secure to the extent that not even company employees can read the contents your emails. Hushmail is known to cooperate with law enforcement by handing over encrypted emails.
7. **Hidden Wiki:** A "hidden service" website on the Tor anonymous network that allows for open editing of subjects related to hidden services and activity in them.
8. **Hub Forums:** An Onion-based platform for cross marketplace discussion, like the Dream Market forum or sub reddit, these forums are usually fully anonymous.
9. **IRC (Internet Relay Chat):** A communication system allowing the easy transfer of text-based messages. It is intended for group discussions in sessions called channels. IRC channels are often used by black markets vendors to provide an update on an arrival of new goods or important massages.
10. **LocalBitcoins:** A site designed to allow over-the-counter trading of Bitcoins. Famed for its anonymous nature, people who sell on the site have been under constant pressure to avoid being prosecuted as unlicensed money traders. This extra risk and the extra work generally cause a significant price difference between the site and a more open (and regulated) exchange.
11. **Marketplaces:** Catch-all term for websites set up to allow trade between vendors and buyers. When used in the context of selling illegal goods, these usually provide anonymity to the buyer and seller, a method of escrow to ensure reduced risk from new vendors and sellers, and a method of advertising goods to be sold at a price so that a purchase may be initiated and paid for without involvement from the seller. Most markets are also set up as 'hidden services' under anonymity networks like Tor, i2p, or Freenet, although there do exist some 'clearnet' markets that operate over standard HTTP/HTTPS.
12. **Onion Browser:** A web browser like the Tor Browser Bundle (TBB). This web browser is designed to work with the Tor network to browse hidden services and normal websites anonymously, without leaking user information. While easier to use properly without

leaking information, bugs in a browser can cause serious problems, such as the javascript bug that was used in part to shut down Freedom Hosting.

13. **SIGAINT:** Tor-based darknet email service that allows you to send email without revealing your location or identity. Its name is derived from SIGINT (“Signals Intelligence”), which refers to intelligence-gathering by intercepting signals.
14. **Torchat:** Instant Messaging service that works by having each user set up a ‘hidden service’ that can be used to contact them via Tor. Somewhat similar in purpose to OTR, but messages do not have plausible deniability.
15. **Tormail:** Tormail was a Tor hidden service that allowed users to send and receive email anonymously and email addresses inside and outside the Tor network. The service was seized by the FBI as part of the Freedom Hosting bust in August 2013.

Knowledge Is Power!

Get access to free sales training on both Cloud Security Services and our revamped ADC sales accreditation. Stay informed about the latest cloud trends and cloud security requirements, so you’re better positioned to beat the competition and increase your business of Radware solutions in 2019.

Learn More

- S1 — Cloud Security Services Sales Accreditation
- S2 — Application Delivery Sales Accreditation

Take Advantage of Affordable Customer Training

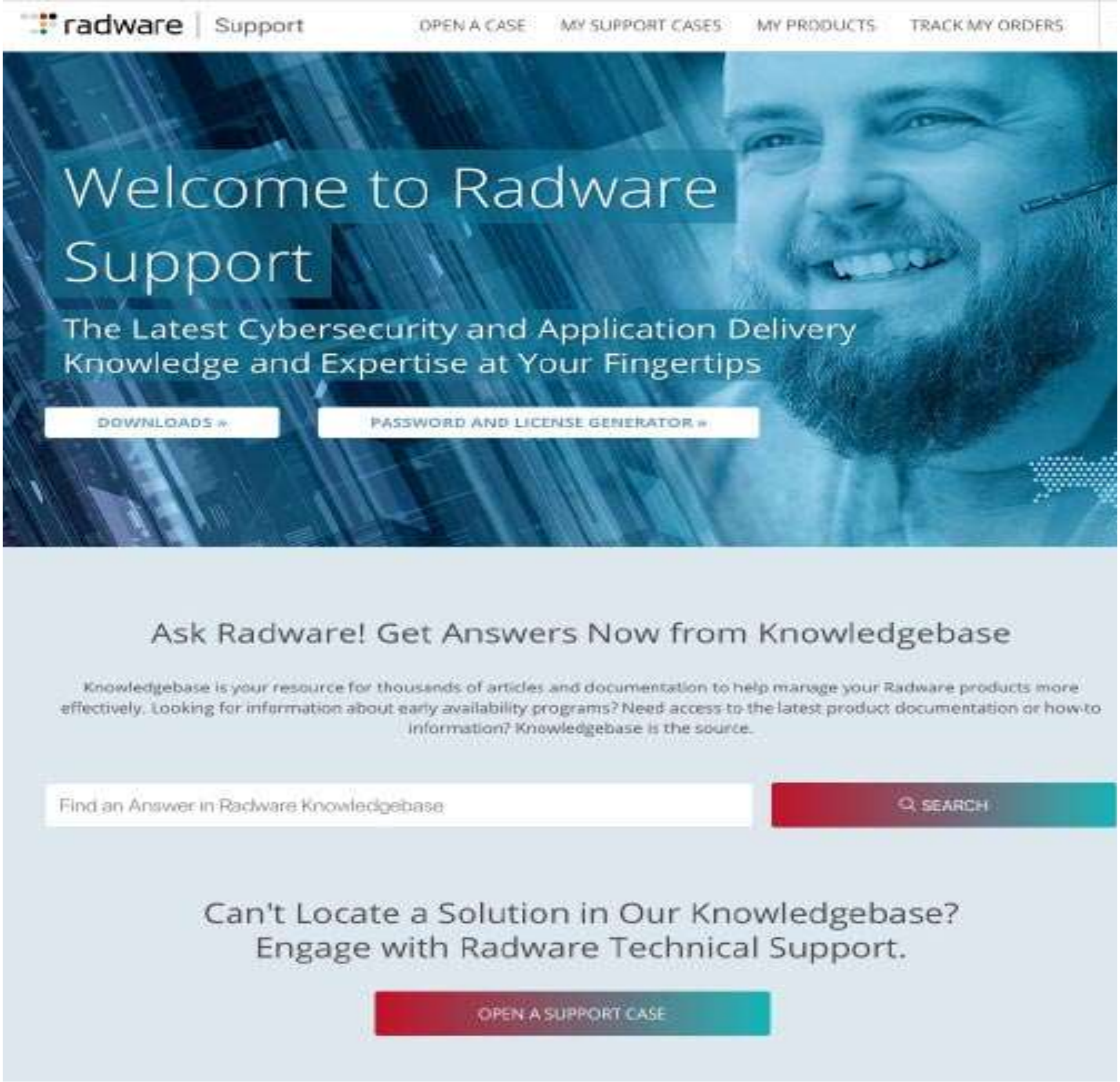
Encourage customers to participate in Radware’s free training programs to learn how to successfully deploy and benefit from our security, cloud and ADC solutions. Customers are eligible for a 20% discount upon completion of one of the free training programs.

Enjoy the free training programs yourself, since they're also available to Radware partners. Visit the customer portal and start your training now!

Take a Fresh Look at the Radware Support Portal

The Radware support portal has been redesigned to provide our customers with a seamless self-service experience. The new and improved support portal helps customers unleash the full potential of their Radware solutions with quick access to the information they need the most:

- **Answers from Knowledge Base** — Gives access to the latest product documentation or how-to information.
- **Password and License Generator** — Allows customers to independently create a software-upgrade password and license 24x7.
- **Easy Access to Downloads** — Provides links to current software versions, release and maintenance notes, and user manuals.
- **Free Online Product Training** — Offers free fundamental courses — available now — in the Learning Academy.



Welcome to Radware Support

The Latest Cybersecurity and Application Delivery Knowledge and Expertise at Your Fingertips

Ask Radware! Get Answers Now from Knowledgebase

Knowledgebase is your resource for thousands of articles and documentation to help manage your Radware products more effectively. Looking for information about early availability programs? Need access to the latest product documentation or how-to information? Knowledgebase is the source.

Can't Locate a Solution in Our Knowledgebase? Engage with Radware Technical Support.

Why Settle? New Akamai Replacement Promotion

Leverage this new replacement promotion targeting Prolexic customers with a custom-built commercial offering that provides better protection at a lower cost.

Get all the tools that you need to get started, including a customer presentation, case study, partner sales playbook, product battle card and much more.