DDoS and DoS Protection in the Medical World Today

DDoS and DOS attacks remain significant problems in the IT industry, particularly in the medical and utility sectors. In these fields, denial of service attacks have become common tools for bad actors to extract ransomware payments. The medical industry has inadvertently played into the hands of these bad actors by.

1. **Moving their previously self-hosted electronic medical record (EMR) systems and other medical applications to the cloud, often to a SaaS offering. There are numerous good reasons for this.**
2. **Deploying volumetric-based DDoS attack protection, which historically protected against the majority of denial-of-service attacks.**

These trends have created a perfect storm of risk for the medical industry, which bad actors have been exploiting. Denial of service attacks have existed since the dawn of the internet. The first recorded denial of service attack was launched against one of the world's original ISPs, "Panix", this attack caused a major service disruption by targeting a specific device's state table. Over the past few years, this type of attack, which does not require high traffic volume and can be triggered from a single attacking machine, has become less common. Instead, distributed denial of service attacks that aim to consume all internet bandwidth have become the main attack vector for bad actors. As a result, most hospitals and other industries have standardized their defense strategies by using cloud services to protect against the majority of attacks.

Cloud Services Deployment

Cloud services are deployed in one of two ways:

1. **Swing Motion**
   Once an attack is detected, the hospital changes its inbound routed traffic to flow through the DDoS protection services. This usually takes a few minutes to activate..

2. **Always On**
   This more expensive option includes always-on protection as traffic always flows through the DDoS protection provider's proxy.

As hospitals moved to SaaS-based DDoS protection, many also transitioned their EMR and other medical apps from self-hosted to SaaS delivery, driven by substantial financial and support benefits. While these choices were not mistakes, they introduced new risk vectors and unintended consequences—most notably, a single point of failure. If a critical device in line to the WAN or internet goes down, the EMR becomes inaccessible, preventing patient care. The once lowly DoS attack has become a growing threat, with previously rare incidents now increasingly targeting hospitals. Bad actors, especially groups like Killnet (a Russian extra-governmental group), have ramped up attacks against the West, heavily targeting medical institutions. They are aware that volumetric DDoS attacks are well-protected, so they have focused on DoS attacks and DDoS pulse attacks (short-lived attacks that exploit the "swing" time to create outages). Cloud DDoS protection vendors struggle to offer protection against DoS attacks because these attacks tend to be small and specifically targeted, requiring very granular protections. The cloud service SaaS DDoS protection offerings can protect against pulse attacks but only if deployed in an always-on model, which is very expensive.

Risk Highlight

To highlight the risk posed by DoS attacks, here are several common vulnerabilities and exposures (CVEs) related to DoS vulnerabilities from leading hardware vendors over the past few years:

Cisco:
1. Advisory ID: cisco-sa-ssh-dos-Un22sd2A (2020 June 3) CVE-2020-3200
2. Advisory ID: cisco-sa-ftd-dos-JnnJm4wB (2022 April 27) CVE-2022-20757
3. Advisory ID: cisco-sa-ssh-excpt-dos-FzOBQTnk (2022 September 28) CVE-2022-20920
4. Advisory ID: cisco-sa-accsc-dos-9SLzkZ8 (2023 November 15) CVE-2023-20240 and CVE-2023-20241
5. Advisory ID: cisco-sa-cucm-dos-kkHq43We (2024 August 21) CVE-2024-20375
6. Advisory ID: cisco-sa-nxos-dhcp6-relay-dos-znEAA6xn (2024 August 28) CVE-2024-20446

Palo Alto Networks:

1. **CVE-2024-3384:**
   https://security.paloaltonetworks.com/CVE-2024-3384
2. **CVE-2022-20757:**
   https://www.securityweek.com/palo-alto-networks-patches-vulnerabilities-allowing-firewall-disruption/amp/
3. **CVE-2020-2040:**
   https://www.tenable.com/blog/cve-2020-2040-critical-buffer-overflow-vulnerability-in-pan-os-devices-disclosed
4. **CVE-2021-3063:**
   https://security.paloaltonetworks.com/CVE-2021-3063
5. **CVE-2021-3053:**
   https://security.paloaltonetworks.com/CVE-2021-3053
6. **CVE-2022-0028:**
   https://security.paloaltonetworks.com/CVE-2022-0028
7. **CVE-2023-44487:**
   https://security.paloaltonetworks.com/CVE-2023-44487
8. **CVE-2024-3382:**
   https://security.paloaltonetworks.com/CVE-2024-3382
9. **CVE-2024-3385:**
   https://security.paloaltonetworks.com/CVE-2024-3385

As you can see, the security devices and vendors we rely on to ensure our connectivity are being exploited to create availability vulnerabilities. The biggest problem for the medical industry is that we now have a single point of failure: the external interface/IP of the router connecting to SaaS apps like EPIC or Cerner.

Recent Denial of Service Attacks on Hospital Systems

1. **Florida Healthy Kids Corporation (2023):**
   Targeted by a DoS attack that exposed over 3.5 million patient records, significantly disrupting services.

2. **UVM Health Network (2023)**
   Experienced a severe DoS attack that disrupted patient care across multiple facilities, leading to system outages lasting several weeks..

3. **Mon Health System (2024):**
   Impacted by a DoS attack affecting more than 492,000 patients, causing the system to go offline and forcing emergency measures.

4. **Wakulla County Hospital (2024):**
   Experienced a DoS attack that temporarily shut down its network, impacting patient care and operations.

5 **Norwood Clinic (2023):**
Suffered a DoS attack that exposed patient information and led to significant operational disruptions.

6 **Southeast Michigan's Henry Ford Health System (2023):**
Hit by a DoS attack that disrupted access to patient records and delayed medical services.

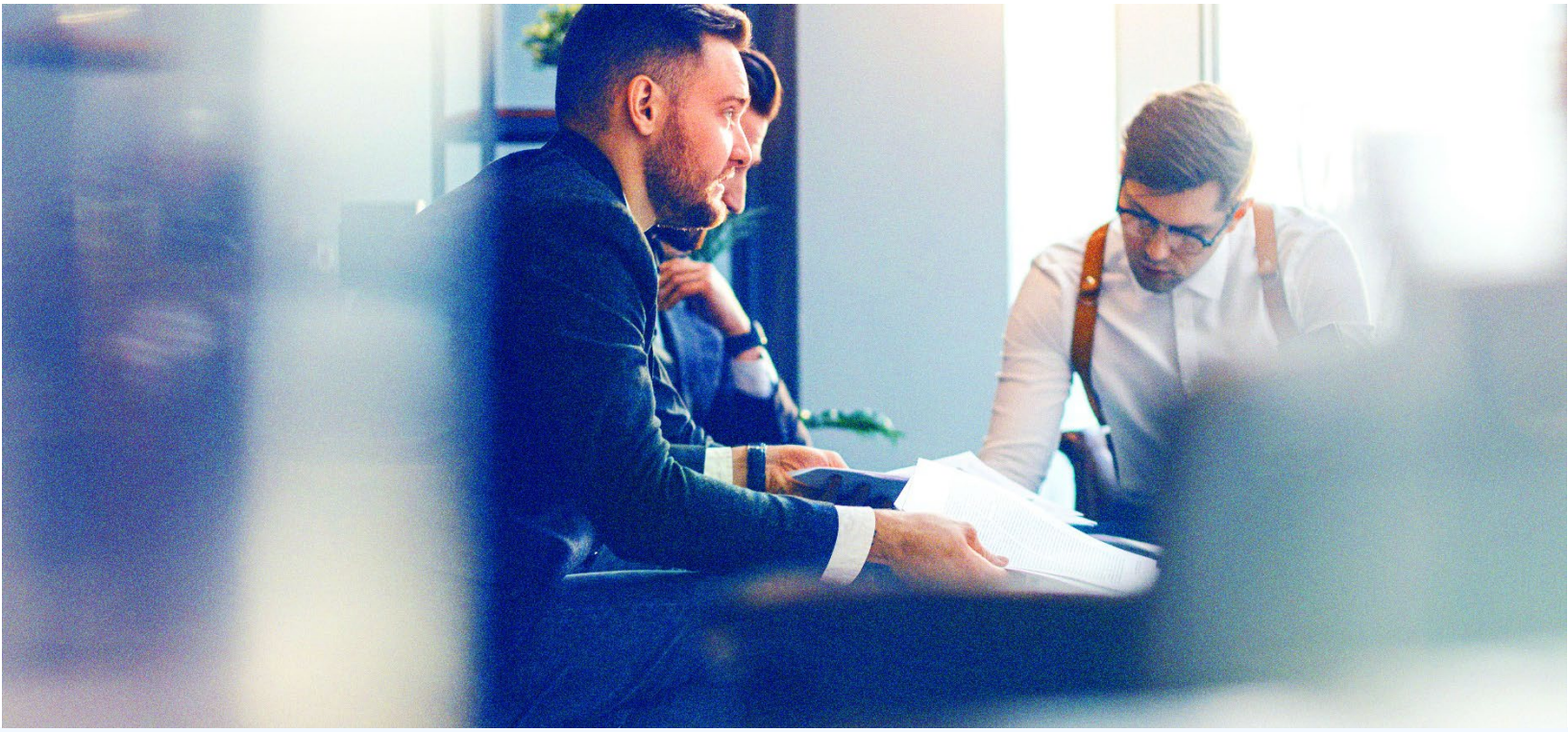
7 **Logan Health Medical Center (2023):**
Suffered a breach including elements of a DoS attack, affecting over 213,000 individuals.

8 **Comprehensive Health Services (2024):**
Experienced a DoS attack impacting over 106,000 people, leading to significant disruptions in patient services.

9 **South Shore Hospital (2024):**
Affected by a DoS attack that exposed personal health information of over 115,000 individuals.

10 **Medical Review Institute of America (2024):**
Suffered a DoS attack compromising sensitive personal information of over 134,000 individuals.

Conclusion



This doesn't mean there aren't solutions or that your current investments are wasted. It means we must stay vigilant, continue to review our protections, and add necessary controls when neeeded. All of us especially medical institutions need to review their DDoS SaaS provider capabilities, how we receive service (swing or always on), ideally add an on prem DDoS/DoS mitigation components. In the perfect world our organizations would be able to deploy an always on SaaS DDoS mitigation architecture coupled to with an on prem DDoS/DoS mitigation capability . In most cases the best and most cost effective solution is likely a hybrid swing architecture where on prem devices mitigate DoS atatcks and provide protection during the time it takes to move traffic between the SaaS protection and the traditional Internet connections.

One thing is for sure: the risk is real, and the cost to protect against this type of attack is minuscule compared to the cost of failing to do so.

SPEAK WITH A SPECIALIST