# Are Periodic Vulnerability Scans Enough to Prevent Breaches?


**Author:**

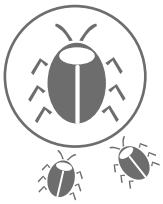
Amarnath Chatterjee,
AVP Product Development,
Paladion Networks

PALADION
HIGH SPEED CYBER DEFENSE

Vulnerability scans are implemented for the purpose of preventing cyber security breaches in the same way a single guard patrols an area to prevent an attack. The guard acts as eyes, but cannot really stop the attack if and when it happens. It's ludicrous to think that knowing about a threat is enough to actually do something about it. The Ponemon Institute of Research submitted a research paper claiming that companies could expect 51 breaches every year despite diligent vulnerability scanning that took place on a regular basis. If this is the case, should CIOs and cyber security teams be implementing more than periodic scans to prevent & remedy attacks?

> "Periodic vulnerability scans simply do not do enough to prevent a breach from happening, or to exercise damage control once it has happened.'"

Once a vulnerability has been detected, a patch can be implemented to bolster cyber security within that virtual section. However, it's possible (and probable) that these patches will only be released months after the initial detection, because adapting to modern attacks is a process that takes time (and installing those patches will cause even further delays). This leaves companies in a position where they know about the vulnerability without being in a position of being able to do anything about it. This gap is a dangerous one because it leaves a company open to attacks. In addition to this, these security vulnerabilities cannot always be isolated or disconnected for long periods of time because they are necessary for normal day-to-day functionality.

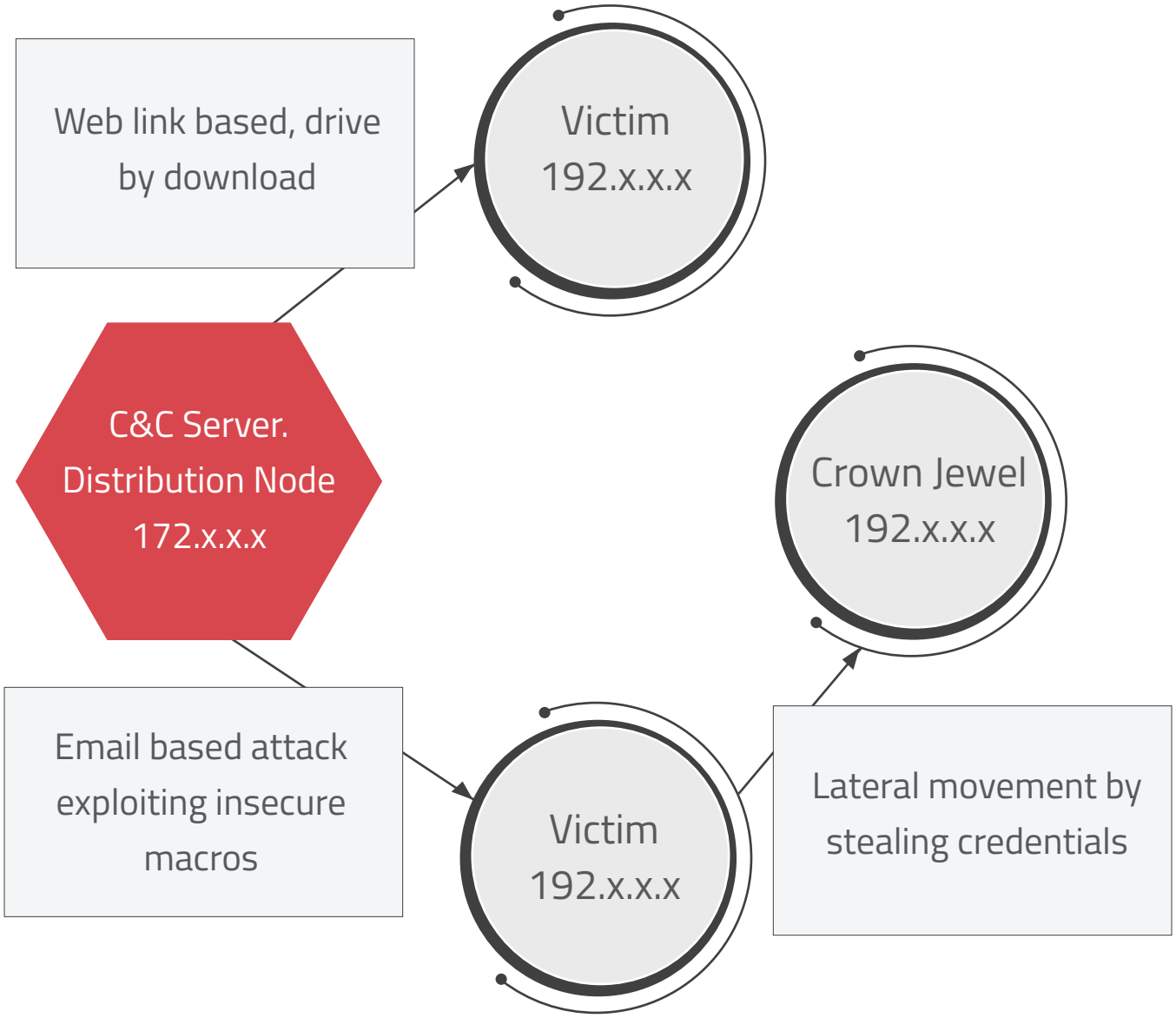


## The Additional Threat of Blended Attacks

Today, one breach may have the ability to attack multiple areas at the same time if they are even slightly vulnerable. This pronged attack strategy is another reason why more must be done to react to threats, because virus authors & hackers are happy to team up for the sake of getting past basic vulnerability scans.

Blended threats such as Nimbda, CodeRed, BugBear and Klez are highly contagious and will rapidly propagate throughout any system if nothing more than a single propagation vector is in place.

Blended threats are usually armed with the ability to take root via multiple footholds such as email attachments, downloadable files, etc. They also have a knack for getting past virtual areas whether these have preventative security or not. In addition to this, blended threats spread quickly and have the ability to hide themselves extremely well. If it wasn't for blended attacks, perhaps vulnerability scanning would be enough; but while threats evolve, so too must cyber defences.

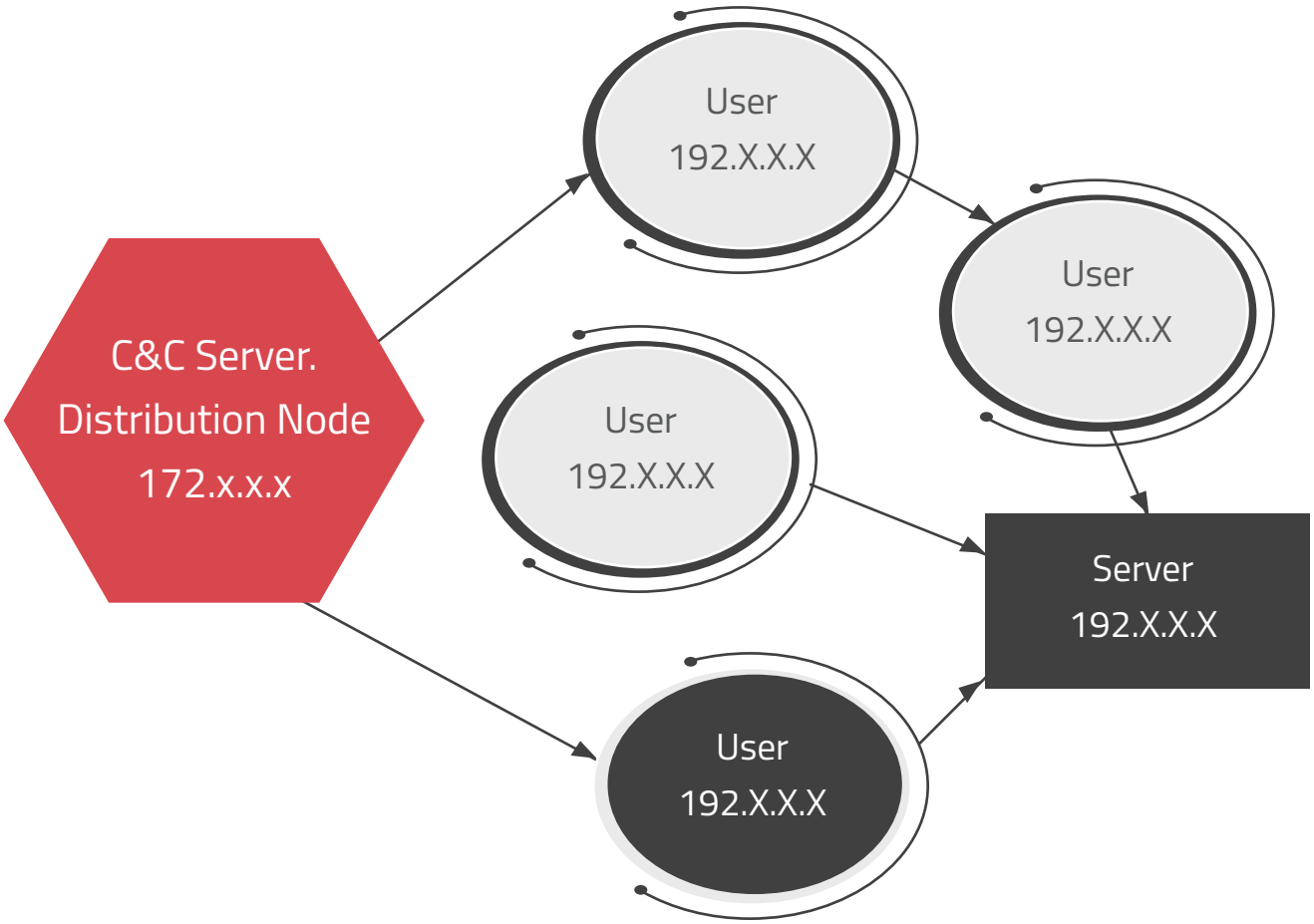


# Single Propagation Security is No Longer Enough Protection

Assuming a system has multiple vulnerabilities, it's safe to say that blended threats are adept at attacking a few specific targets instead of all of those vulnerabilities; in order to remain relatively undetected. This creates an infection chain which makes exploitation that much easier. Vulnerabilities can therefore be divided into two categories; hot zone vulnerabilities and cold zone vulnerabilities. The hot zone vulnerabilities are sections where threats are actively taking place, and the cold zone vulnerabilities are areas where there are no threats at all.

Instead of following conventional security measures where hot zones and cold zones are treated the same (single propagation security), it's more effective to focus in on the hot zone infection chain so that all resources are concentrated on the real threat.

"Adequate cyber security requires more than simply assessing vulnerabilities. Infection chains must be identified and prevented or real time containment will be impossible."

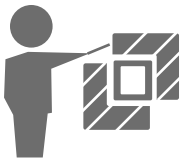



# How to make use of Indicators of Compromise

If endpoints have loopholes, malicious threats will easily gain a foothold and use that foothold to spread & attack. For this reason it's imperative to have a system in place that can identify indicators of compromise. When a virus or hack exploits an open endpoint successfully, that virtual area will exhibit an indication of compromise. These must be visible to the cyber security system in place as well as to the CIO & his/her cyber security team. Successful identification allows these security teams to act quickly and more effectively once a threat has become apparent.

A vulnerability assessment must be coupled with a secure configuration assessment in order to be effective. Add to this a process that identifies indicators of compromise and the result is a system that can prevent as well as remedy any breach attempt. This is the only way to protect a system where endpoints are interconnected throughout the entire system. Even though a non-critical point is being less protected than a critical point, the threat may start at the non-critical point and work its way up to the critical point without being detected. A dynamic approach such as the one described above is the only way to prevent this from happening. Malicious behaviour is tracked and the threat is averted because the interconnected pathway is prioritised over actual endpoints where threats are either started or where they are attempting to end up. The pathways are where the real battle is won and lost.

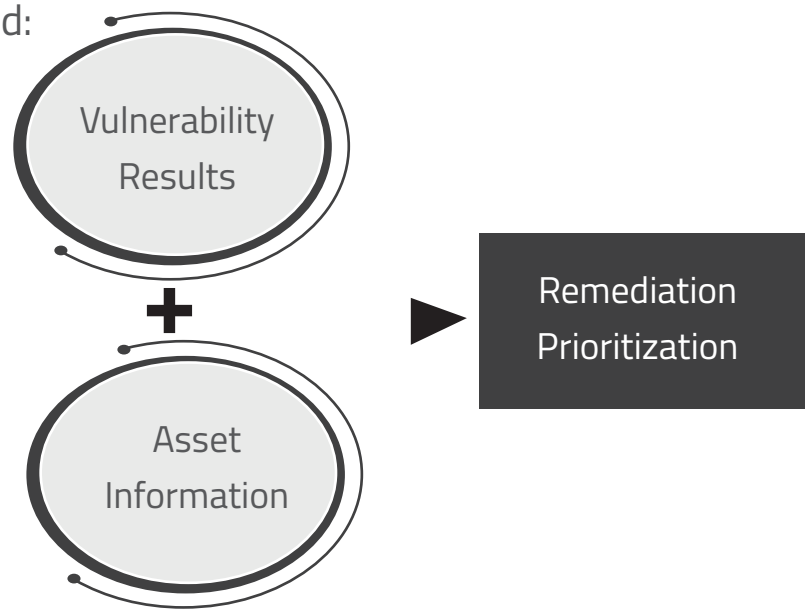
Vulnerability Assessment + Configuration Assessment + IOC Detection



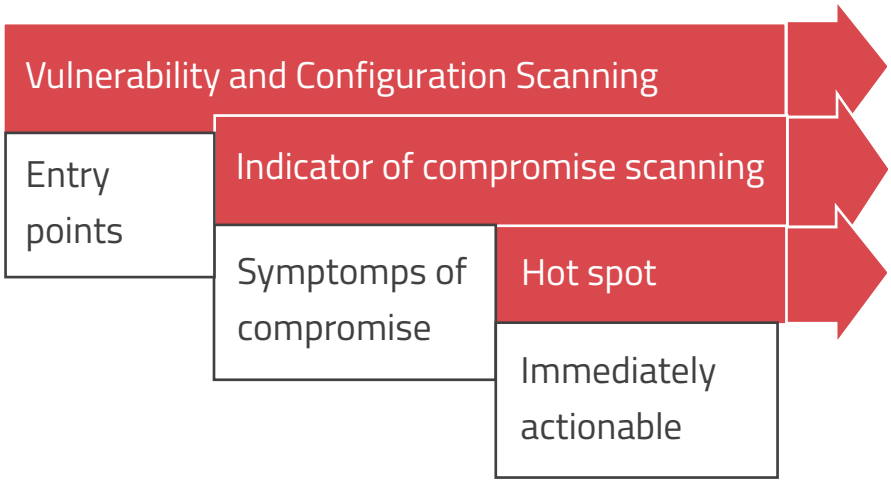
# Recognising the Difference Between Hot Spots and Hot Zones

A hot spot can be simply defined as an area or endpoint that has been compromised by a threat. Basic prevention and vulnerability scans have been designed to protect these areas as well as notify security if a breach has taken place. Here is a comparison between the old way of dealing with these threats versus the new way.

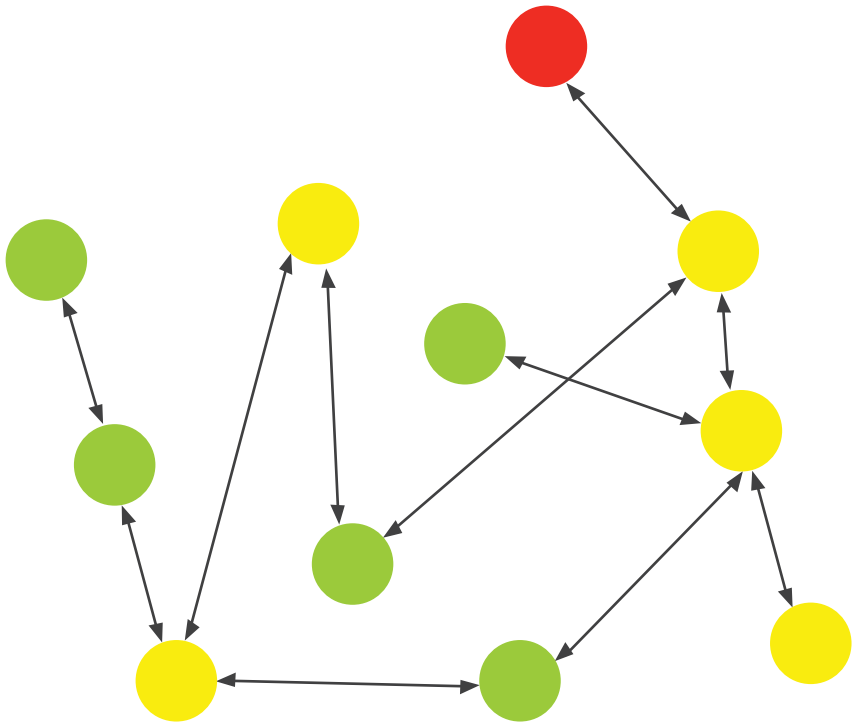
Old method:



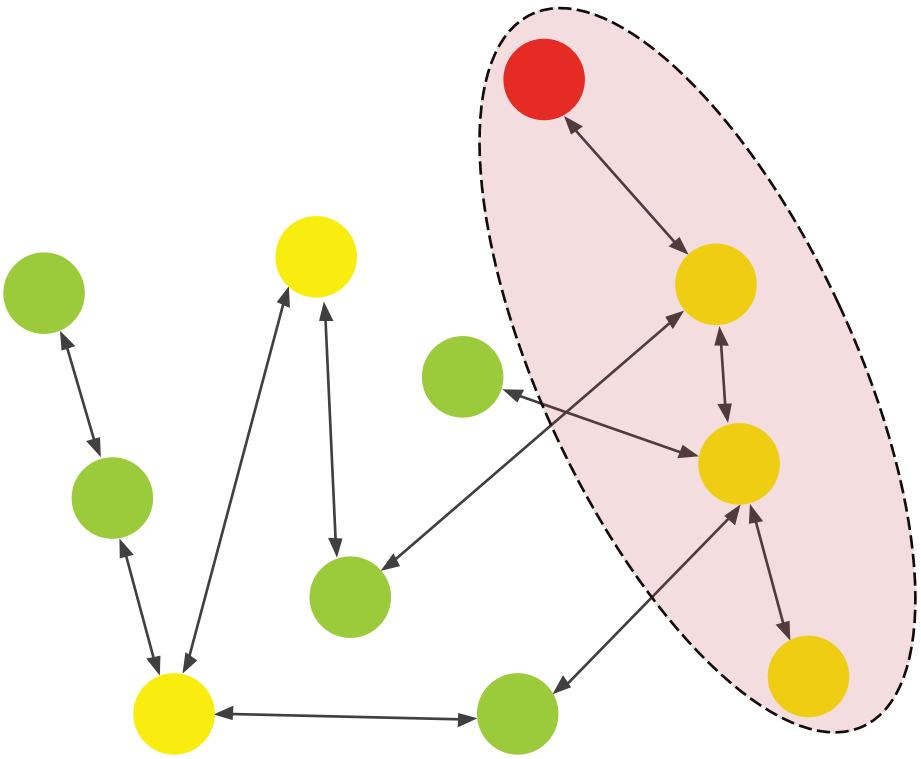

New method:




More importantly, however, a hot zone is an interconnected pathway—from one endpoint to another—that has been compromised by a malicious threat. This is where real time protection can and should take place. Identifying hot zones quickly will allow cyber security teams to deal with blended threats rapidly and more effectively.



If the green dots represent endpoints that are safe from threats, while the yellow dots represent endpoints that are at risk, it's clear that a hot zone exists. Identifying this hot zone is a vital part to the remedy and requires the ability to see the compromised endpoint (represented by the red dot), and how this endpoint may affect other areas.



# Conclusion

The processes of vulnerability scanning and the gathering of asset information are essential parts of cyber security, but they are only the beginning. More measures must be taken to prevent modern attacks such as blended threats which are being devised by hackers and virus authors. By monitoring the entry points and endpoints of a system, all that is accomplished is basic vulnerability remediation—a process that is not quick enough to effect real time protection. Since blended threats do exist and are on the rise, a new way of defense is clearly called for.

*The solution therefore lies in a three-pronged defense that includes a vulnerability assessment, a secure configuration assessment, and an effective method of indicating compromises. Once all three of these methods are in place, effective security can stop threats in their tracks because hot zones are easily identified, contained, and remedied. Affected pathways between entry points and endpoints are therefore focused upon while cold zones are ignored as non-critical. This allows CIOs and their teams to effectively intercept a threat before it propagates itself further into the system.*

*This three pronged defense can is available in Paladion's RisqVU IST. You can request for a demo of the product or take a free trail by visiting here: http://paladion.net/risq-vu-ist/*

PALADION
HIGH SPEED CYBER DEFENSE

## ABOUT PALADION

Paladion is a global cyber defense company that provides Managed Detection and Response Services, DevOps Security, Cyber Forensics, Incident Response, and more by tightly bundling its semi-autonomous cyber platform and managed services with leading security technologies. Paladion is consistently rated and recognized by independent analyst firms and awarded by CRN, Asian Banker, Red Herring, amongst others.

For 17 years, Paladion has been actively managing cyber risk for over 700 customers from its six cyber operations centers placed across the globe. It houses 900+ cyber security professionals including security researchers, threat hunters, ethical hackers, incident responders, solution architects, consultants and more. Paladion is also actively involved in several information security research forums such as OWASP, and has authored several books on security monitoring, application security, and more.

---

**WW Headquarters:** 11480 Commerce Park Drive, Suite 210, Reston, VA 20191 USA. Ph: +1-844-507-7668

Bangalore: +91-80-42543444, Mumbai: +91-2233655151, Delhi: +91-9910301180, London: +44(0)2071487475, Dubai: +971-4-2595526, Sharjah: +971-50-8344863, Doha: +97433559018, Riyadh: +966(0)114725163, Muscat: +968 99383575, Kuala Lumpur: +60-3-7660-4988, Bangkok: +66 23093650-51, Jalan Kedoya Raya: +62-8111664399.

sales@paladion.net | www.paladion.net