ARBOR NETWORKS

Security Current Whitepaper

# Attack Campaigns: Connecting the Dots to Disrupt the Adversary

securitycurrent

*"Patience and perseverance have a magical effect before which difficulties disappear and obstacles vanish." – John Quincy Adams*

**Adversaries have patience and expect to persevere over any and all obstacles that stand in front of them. Their toolkit is not limited and if at first they don't succeed they'll try again until they complete their mission. The enterprise's challenge: find and disrupt them before they fulfill their mission and prepare for the next one, never relinquishing their hold.**

Cybersecurity threats to the enterprise continue to move at a pace whereby many organizations are not able to keep up with the known, let alone advanced adversarial tactics. For years the industry has concluded that advanced attacks involve some sort of malware in order to be successful. While malware can be used to exploit a target, there's an evolution occurring that extends beyond the need for malware or zero-day exploits: attack campaigns. An attack campaign is not just an opportunistic attack aiming to compromise an endpoint, but rather a deliberately focused effort with a specific motive and mission with the intention to persevere until the campaign's successful conclusion.

Well-funded, calculated, and with a specific motive, the adversaries may be nation-states, organized crime, terrorists, or hacktivists. Attack campaigns represent one of the most serious forms of organizational risk and defeating them requires the support and visibility of senior officials and boards within the company. The impact isn't just an infected host and subsequent cleanup; it is instead a succeed-at-all-costs campaign designed to bypass modern-day defense capabilities to exfiltrate intellectual property or destroy infrastructure to gain a competitive advantage. With an average dwell time of 205 days[1] before discovery, organizations need to uncover clues and draw conclusions more quickly. Traditional solutions are too slow, with latent workflows or littered with false positives leading to alert fatigue. By the time the alert triggers, the adversary has achieved the mission.

An attack campaign is not just an opportunist attack aiming to compromise an endpoint, but rather a deliberately focused effort with a specific motive and mission with the intention to persevere until the campaign's successful conclusion.

### The State of an Enterprise

Piecing together unusual events that are, in a manner of speaking, hiding in plain sight, is inundating security teams. Hindsight is always 20/20 and replaying an attack after discovery typically ends with analysts truly understanding how attackers were successful. However, connecting the dots in the heat of the moment has left too many Security Operations Centers (SOCs) focused on the wrong events. With businesses eager to gain a competitive advantage, security typically isn't a business strategy priority. As a result, security teams find themselves faced with a complex environment, which may not be well documented, trying to understand what connections are legitimate and which are worthy of investigation. When this occurs, connecting the dots of an attack is challenging. Attackers remain resident on the network and security teams can't identify the problem because they're lacking the skillset and solution to hunt when it's necessary and not just when it's too late.

Security teams face the aforementioned demands in the midst of their own challenges of a maturing organization and the struggle to retain security talent. Entry-level security staff members are expected to come up to speed quickly and once they do they are very marketable. As such, security leaders invest heavily to prepare analysts and then fight to retain them to avoid repeating this expensive cycle. In the event security leaders decide to outsource to a managed security service provider (MSSP) due to staffing issues, it does not eliminate their responsibility to protect what they have been entrusted to safeguard. Vendors must provide solutions for analysts to reduce attacker dwell time from months to minutes.

### Adversary Advancements

Security leaders and their teams spend many hours on vulnerability management and privileged account management to plug as many holes as possible to reduce their attack surface and improve their security posture. Organizations deploy firewalls, IDS/IPS, malware sandboxes, endpoint detection and response solutions, and other technical controls as components of a defense-in-depth strategy. Yet attackers are still breaching organizations and remaining undiscovered for extended periods.

[1]https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf

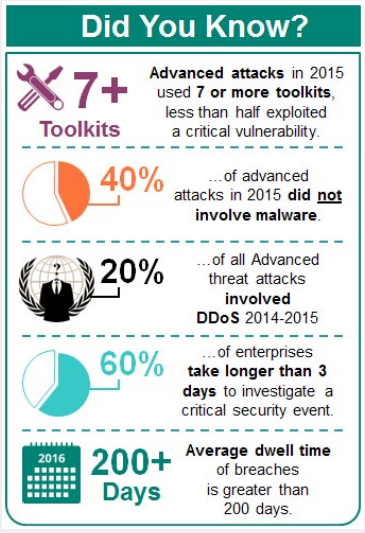


*Figure 1 – Adversary Advancement Data*

The adversary's campaign is one with endless tactics to evade prevention and detection solutions. They will perform their reconnaissance and diligently work with a well-funded team until their mission is complete and with little expectation of being caught in the process.

Adversaries expect to encounter the latest security controls such as endpoint detection and response solutions, next-generation firewalls, and anti-malware sandboxes protecting the business. The fact is adversaries have evolved their tactics to rely no longer on known vulnerabilities hoping to find unpatched hosts. Adversaries don't need to leverage advanced malware to be successful; a simple credentials theft will do just fine. Not relying on vulnerabilities or advanced malware dramatically reduces the likelihood of tripping an alert, which makes identifying malicious activity inside the perimeter defenses so difficult. To address this gap, it is important to have intuitive and advanced intelligent search capabilities for enterprise analysts of all levels, from entry-level to seasoned professional.

### Modern Day Attacks, but Yesterday's Defenses

Complexity remains the enemy of security. Furthermore, employees are the favorite target of the attacker. Additionally, the business has more turnkey solutions at their disposal than ever before, and they don't need to engage IT or security to deploy them. The business is not going to slow down for security and it will enable SaaS solutions, partner with third parties, and cobble together the best of what the market has to offer in order to gain a competitive advantage. Making it easy for employees, keeping costs down, and supporting the organization's strategic direction makes business sense. Security teams haven't lost complete control, but their ability to manage data and access while keeping external and internal threats minimized is increasingly challenged.

There is no shortage of innovation and spending in cybersecurity with a worldwide market projected at $170 billion by 2020[2]. In 2015 alone[3], venture-backed cybersecurity companies raised $1.9 billion globally with many aiming to solve advanced threats. The industry can expect that no matter what defenses are deployed; attackers will work feverishly to find their way around the obstacles.

Many large complex companies have substantial investments in security solutions, which will remain within their infrastructure for years to come. For example, security information and event management solutions (SIEMs) are a core component in the SOC and the incident response workflow. Yet SIEMs require a tremendous amount of effort to implement and tune at the onset as well as throughout the plethora of changes that occur with new applications and connections. To that end, SIEMs have been criticized for alert fatigue or lack of timeliness of critical event alerts leading to data exfiltration. Traditional SIEMs often do not detect adversary attack campaigns due to not correlating the data well or quickly enough. Attackers avoid detection and leverage the command and control (C2) and Botnet infrastructure without impediment.

…SIEMs have been criticized for alert fatigue or lack of timeliness of critical event alerts leading to data exfiltration. Traditional SIEMs often do not detect adversary attack campaigns due to not correlating the data well or quickly enough. Attackers avoid detection and leverage the command and control (C2) and Botnet infrastructure without impediment.

### Stages of Attack

A little reconnaissance and some cleaver social engineering leading to credential compromise may be all that it needed to gain a foothold into the business' infrastructure. How big of a concern is credential theft with security professionals? A January 2016-published[4] research report from Rapid7 indicates 90% of security professionals rate that compromised credentials are a top concern. Once the attacker has infiltrated the network they'll move laterally, making detection that much more important before they get a chance to complete their mission. A successful attacker will seek employee, service account, and third-party credentials over malware and zero-day exploits because leveraging access with authorized credentials is harder to detect. This is all the more reason for solutions to identify the earlier stages of attack to reduce the likelihood of a breach.

[2]http://www.csoonline.com/article/2946017/security-leadership/worldwide-cybersecurity-market-sizing-and-projections.html
[3]http://www.wsj.com/articles/vcs-pour-money-into-cybersecurity-startups-1429499474
[4]http://www.rapid7.com/company/news/press-releases/2016/rapid7-research-study-finds-compromised-credentials-top-concern.jsp

Reconnaissance, patience, the will to succeed, and endless funding are attributes associated with the focused attacker. Lockheed Martin's Cyber Kill Chain®[5] illustrates the criticality of disrupting the attacker as early into their mission as possible. If any part of the kill chain is disrupted the adversary's mission fails. Lockheed Martin outlines the kill chain through seven phases:

1. **Reconnaissance** – Research the target (for example) harvest email addresses;
2. **Weaponization** – Create an exploit to deliver (*Note - malware or an exploit is not required if access is gained through compromised credentials. As employees reuse credentials elsewhere, the ability to obtain the access can come from a completely unrelated entity);
3. **Delivery** – Vector such as email and websites (if using an exploit);
4. **Exploitation** – Victim OS or application is exploited, but could also be in the form of compromised credentials. Again, malware is not required;
5. **Installation** – In the case of malware, installation on the asset;
6. **Command and Control (C2)** – Infected host(s) beacon outbound to C2 network;
7. **Actions on Objectives** – Data exfiltration and mission accomplished with persistence maintained.

The anatomy of an attack by a stealthier adversary shows where an attacker is best able to move within the network undetected. After carefully obtaining access to avoid detection, the adversary moves (stage 4) to seek out sensitive data before connecting to the C2 network, exfiltrating the target information. At this point sensitive business information is compromised.

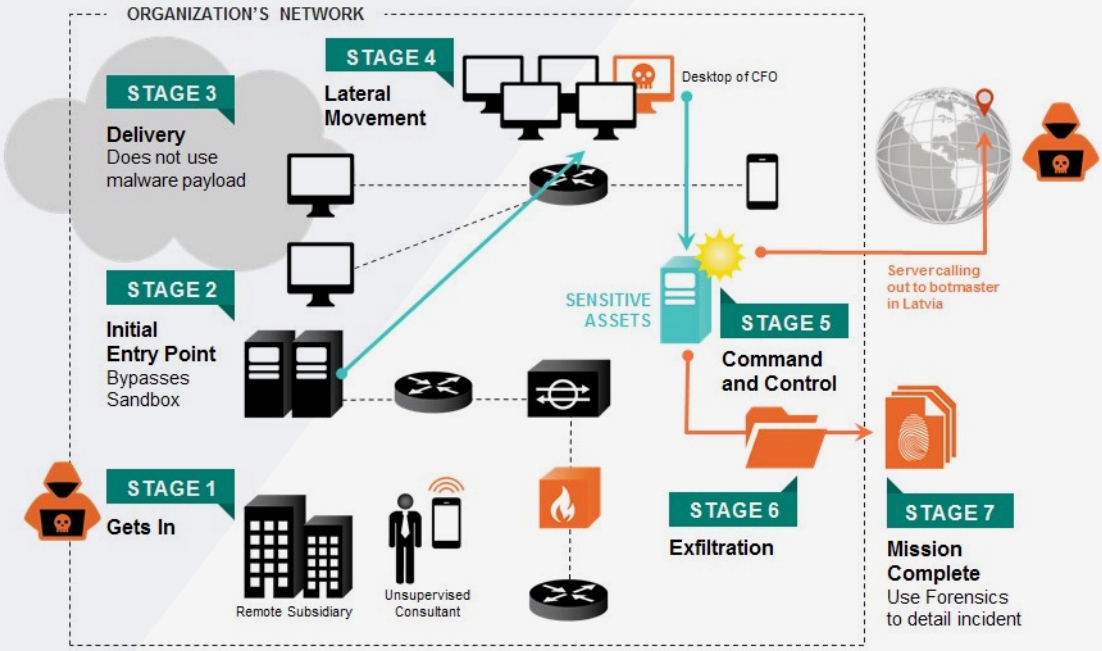


*Figure 2 – The Anatomy of an Attack Campaign*

Going on the offensive, which is not about hacking back in the context of this paper, provides the opportunity to uncover the attacker's activity and disrupt their mission. Essentially this is about taking an active role in finding or hunting for the attacker. The U.S. military defines several steps in its process that can carry over to security teams' ability to detect an intruder[6]: find, fix, track, target, engage, and assess. The find and fix steps speak to actively hunting the attacker as opposed to passively waiting for an alert. Security teams can then take meaningful data refined from intelligent security solutions and turn it into actionable intelligence to disrupt the adversary's mission. Without this intelligence, security teams will miss the opportunity to protect the businesses' sensitive assets. However, with this intelligence security teams identify both system vulnerabilities and locations to begin the hunt, as well as tactics an attacker is likely to use and the steps the attacker took to laterally move through the network.

[5]Lockheed Martin's Cyber Kill Chain http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
[6]Lockheed Martin's Intel Driven Defense Paper http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

**Strategy Must Change – From Perimeter Defense to Hunting**

Playing defense typically consists of combining many solutions together to detect suspicious activity: enable logging, point to a central repository, analyze the logs, and alert when activity is out of tolerance. As previously indicated, the adversary expects to go around many defenses to complete the mission. Furthermore, while it seems ideal to enable as much as possible, the problem is the volume of resources required to manage the applications generating traffic and their SIEM for normalization. For this reason, Arbor Networks has introduced Spectrum – a solution to connect the dots to identify adversaries and disrupt their mission well before a critical alert would have fired. Spectrum aims to turn traditional network defense on its head. To increase analysts' effectiveness, streamlining activity is crucial. Why? To allow for more time to hunt for the adversary. No one likes to admit defeat, but realistically the attacker will penetrate the network, if they are determined, which leads to the need for new approaches like Arbor Networks Spectrum.

…Arbor Networks has introduced, Spectrum – a solution to connect the dots to identify adversaries and disrupt their mission well before a critical alert would have fired. Spectrum aims to turn traditional network defense on its head.

Hunting, as described in Arbor Networks and Security Current's previous whitepaper[7], centers around allocating time for analysts and incident responders to search for traces of an attacker on the network and disrupt the mission before damage is done, rather than waiting for the alert. Streamlining analysis to reduce excessive activities will result in more time to hunt. While some may argue for enabling more systems and logs to identify what has not been discovered, the problem is that security has been doing this for years and breaches are still occurring. Therefore, hunting for the adversary is advantageous because it uncovers incidents that have not created alerts given their slow-and-low tactics. There is a need to incorporate the use of security intelligence with robust search capabilities so that analysts can disrupt the adversary much earlier in the Kill Chain.

As previously defined by Arbor Networks and Security Current (Security Analytics: A Required Escalation in Cyber Defense)[8], security intelligence is "any information that indicates an attack in progress or already successful." Underutilized network traffic correlation can miss valuable Indicators of Compromise (IOCs) to assist with telling the story of what has occurred or is occurring. With lateral movement and C2 heavily involved in the mission, network traffic is a rich source of infrastructure information capable of leading the hunter down the path to disrupt the adversary. Together, analytics and intelligence provides teams with the resources they need to hunt for problems.

Underutilized network traffic correlation can miss valuable Indicators of Compromise (IOCs) to assist with telling the story of what has occurred or is occurring. With lateral movement and C2 heavily involved in the mission, network traffic is a rich source of infrastructure information capable of leading the hunter down the path to disrupt the adversary.

Imagine the ability to model the global Internet. No single enterprise can see enough traffic to uncover all global IOCs. However,worldwide visibility with escalation capabilities is critical to detect lateral movement and anomalous activity matching identified global threat actors and indicators.

Supporting 100% of tier-one service providers, Arbor Networks bring this visibility to the enterprise through Spectrum. Arbor Networks' customers have insight into:

| | | | |
|---|---|---|---|
| IOCs | DDoS Activity | Internet ASN & BGP | Botnet Campaigns |
| Threat Intelligence | Full Packet Captures | Network Anomalies | Low Severity Indicators |

[7] http://pages.arbornetworks.com/website_SEC_Current_Hunted_becomes_Hunter.html
[8] Security Analytics: A Required Escalation in Cyber Defense http://pages.arbornetworks.com/website_ITHarvest_SecurityAnalytics.htm

As referenced in figure 3 below, Arbor Networks has built upon years of blue-chip carrier deployments, an experienced research team, and strategic acquisitions with global visibility, as they innovated with the development of Spectrum. Arbor Networks Spectrum builds upon a nearly two-year ground-up investment and brings Arbor Networks ATLAS intelligence indicators, and their ASERT security research, and content enrichment of global threats, to a single platform with robust search capabilities. Analysts can search and identify potential threats in mere minutes. When analysis is running across terabytes of data and full packet captures, time is of the essence.

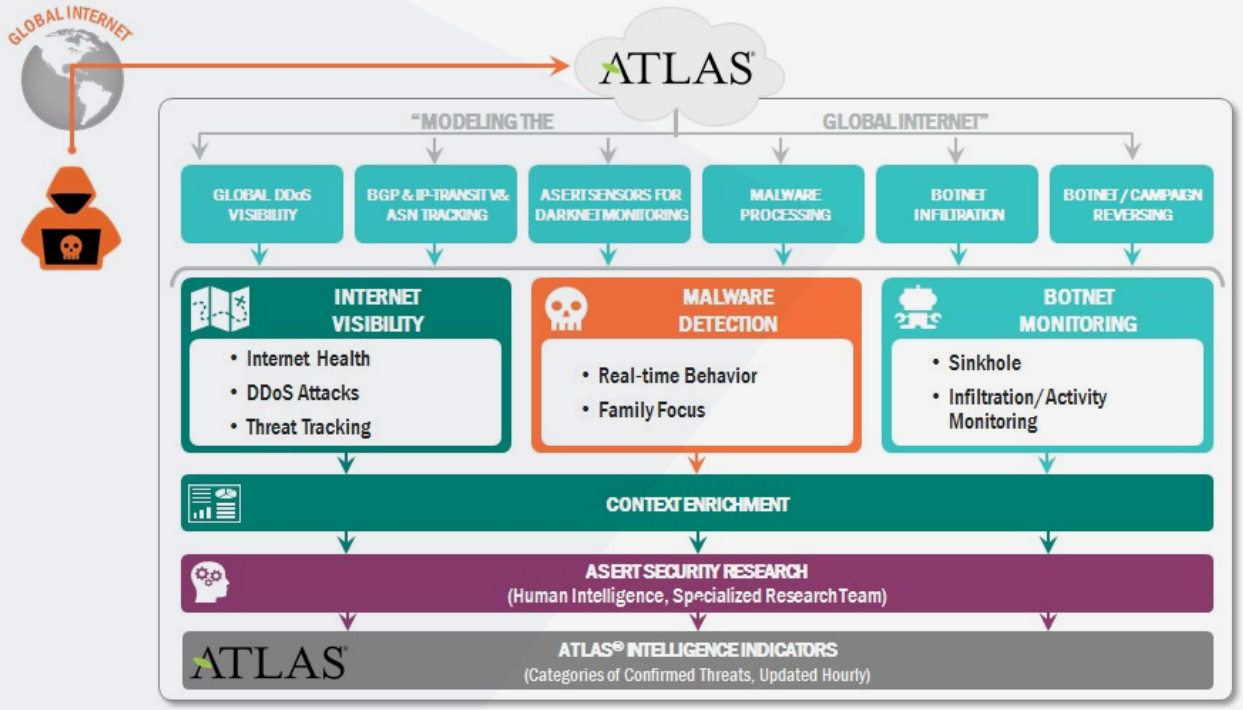


*Figure 3 – Modeling the Global Internet*

**The Analysts Now Add More Value**

Organizations need new-hire analysts to provide value quickly. With the current security job market at near zero unemployment[9], security professionals have no trouble finding work. The challenge security leaders have is not only finding security professionals, but also retaining them. Security professionals advancing their skill set creates plenty of opportunities for new endeavors. Therefore, for example, junior analysts need to contribute value quickly. The solutions they are tasked with administering need to be intuitive enough for analysts to quickly adjust to the learning curve and contribute to the organization. As such, analysts need solutions to help them uncover what may appear to be trivial but ends up significant, and they shouldn't merely focus on the here and now events. Rather, solutions must help analysts understand ongoing activities and not just single events, with the context behind the here and now to tell the story about how it got here. This requires a new solution to enhance the analysts' effectiveness against an attack campaign. With the change in threat type, analysts must be capable of acting much quicker and not relying on passive indicators that may alert as critical events too late.

Solutions aimed at helping organizations disrupt attack campaigns should support a highly visible and intuitive interface, followed by a workflow engine to analyze at the speed of the analyst's thoughts. Collaborating analysts will flip from one possibility to the next very quickly and need solutions to help keep them focused on the path they are on or quickly change and focus elsewhere. Arbor Networks set out to solve this challenge with Spectrum.

[9]http://www.networkworld.com/article/2889203/cisco-subnet/0-cybersecurity-job-unemployment-in-washington.html

Figure 4 below represents the insight an analyst will have when researching integrity of a host.

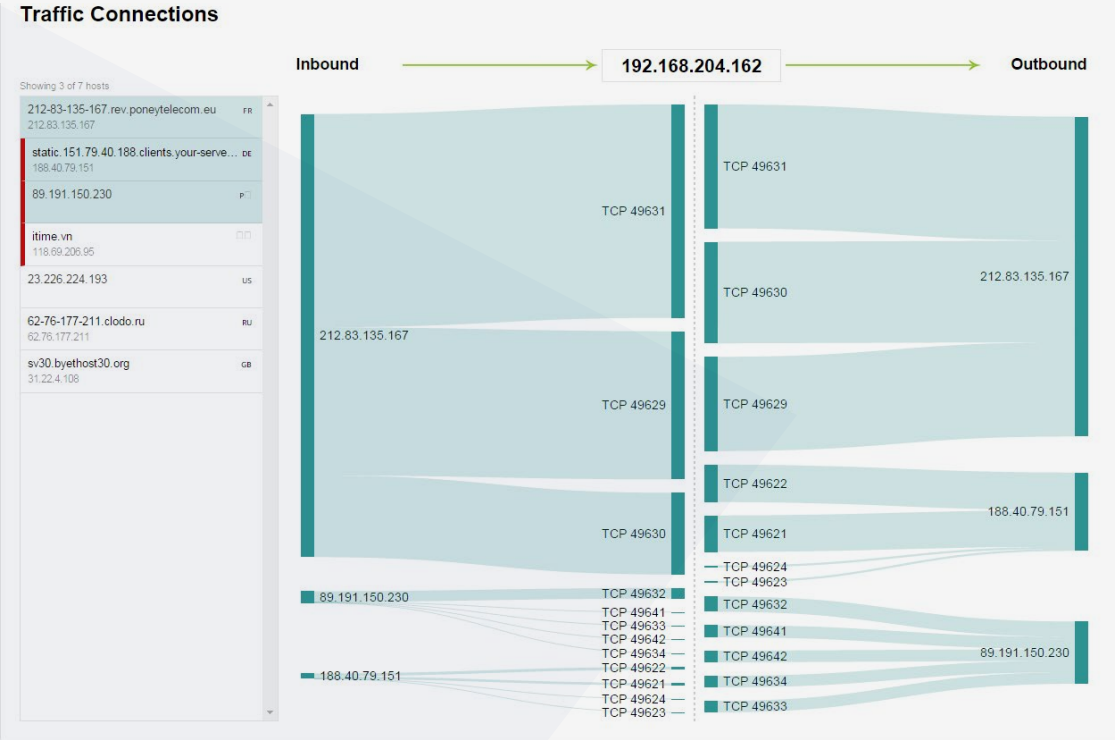


*Figure 4 – Spectrum: Reviewing the Integrity of a Known Host*

Connecting the dots to disrupt a botnet can take years of experience, but with the right solutions, an entry-level analyst can quickly bring value to the security team. Many solutions on the market often have the ability to solve one portion of the puzzle, but not everything in its entirety. This requires analysts to jump back and forth between solutions, hoping no crucial pieces are missing. The reality is this fragmented approach is not effective. Arbor Networks Spectrum helps improve the analysts' effectiveness by uniformly chaining events and traffic, past and present.

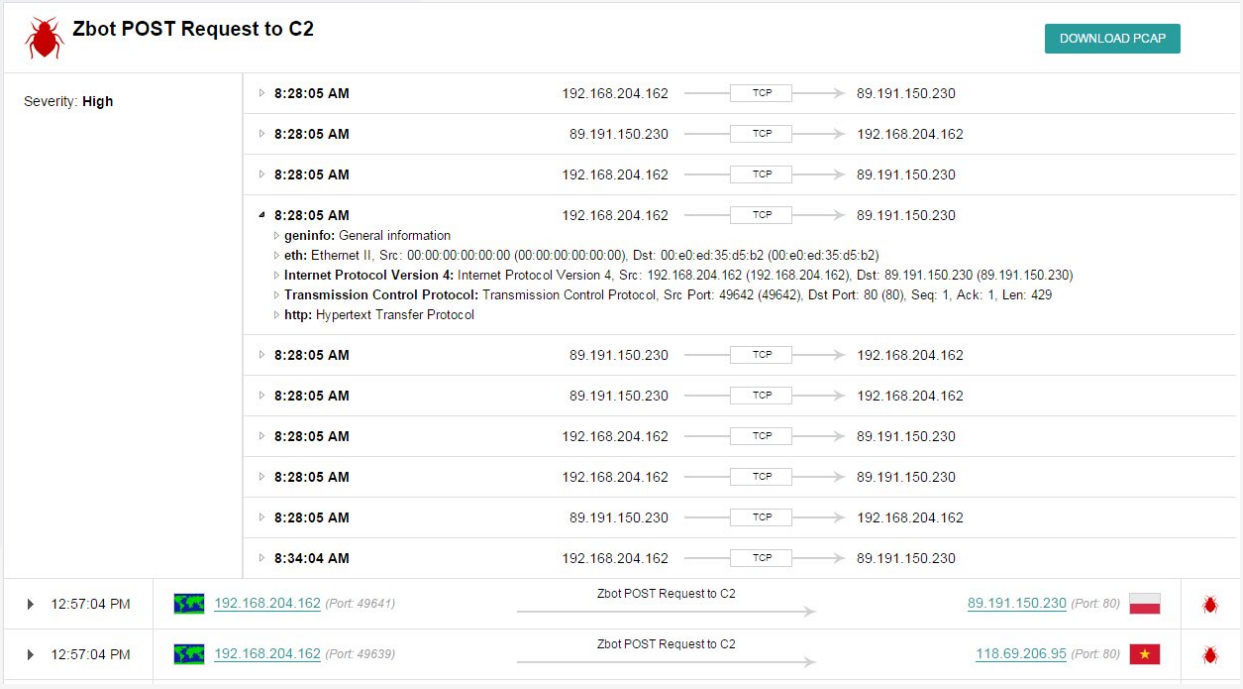


*Figure 5 – CnC Search Detail*

**Why? Attackers Have Advanced, Now We Must Evolve**

Against attack campaigns, security teams must actively connect the dots and not passively wait for the critical alert that may never come from internal systems or may come from a third party but only after data exfiltration. The need for traditional defenses will not dissipate, but there needs to be some change internally to allocate time for security teams to go on the offense and hunt rather than just relying on perimeter control and enabling alerting. Operational teams need time to hunt for the adversary. Stopping the attack from the onset is the goal. However, given the uptick in breaches year over year, security teams must recognize more opportunities through hunting and solid search capabilities to connect the dots and thereby present a highly visible indication as to what occurred, when, and where.

Arbor Networks Spectrum produces actionable data from powerful analysis in minutes as opposed to hours or days. Even the best security teams can be reduced to a subpar operation if their solutions present misleading, wrong, or depreciated indicators. Make no mistake about it; this requires a mindset change from waiting for the alert to proactively hunting. Arbor Networks Spectrum uses its insight across the globe to provide analysts, entry-level or advanced, the ability to pivot and determine the attacker's steps.

Make no mistake about it; this requires a mindset change from waiting for the alert to proactively hunting. Arbor Networks Spectrum uses its insight across the globe to provide analysts, entry-level or advanced, the ability to pivot and determine the attacker's steps.

As the adversary moves within the network, artifacts of the activity remain that solutions like Spectrum can bring to the forefront. In turn, this intelligence allows disruption of the attacker's actions earlier in the Kill Chain. Many traditional network defenses cannot provide this timely information. The defensive change Arbor Networks Spectrum provides begins to turn what the industry has been doing for years on its head. Change is necessary given the incidents in the past and our need to get better at the profession. This is not suggesting that organizations are not trying hard and allocating resources, because they are. The issue is that far too many solutions respond and alert only when it's too late, or were so excessive that teams dealt with alert fatigue. Allocating more people to the problem is not near as effective as a shift to a strategy of hunting.