paloalto NETWORKS

ADVANCED THREATS REQUIRE ADVANCED DEFENSES

Taylor Ettema of Palo Alto Networks on the Key Capabilities Needed in Response

ISMG INFORMATION SECURITY MEDIA GROUP

Taylor Ettema

Ettema is Vice President of product management for internet security at Palo Alto Networks, the network security company that pioneered the next-generation firewall. He has managed a broad range of cloud-delivered security products including network intrusion prevention, malware sandboxing, web security and threat intelligence products throughout his over 10 years with the company. Before joining Palo Alto Networks, Ettema was a principal software engineer and principal investigator for electronic warfare research and development programs for Raytheon Space and Airport Systems in California.

Double-extortion ransomware. Supply chain attacks. Weaponized zero-days. It's an advanced threat landscape, and it requires advanced defenses. **Taylor Ettema** of Palo Alto Networks outlines the key capabilities today's security solutions require to step up against the adversaries' ongoing innovation.

In this video interview with Information Security Media Group, Ettema discusses:

- The evolving threat landscape;
- Where adversaries are taking advantage of defensive gaps;
- Security capabilities required as part of modern defense.

"Adversaries are getting ever more adept at hiding attacks so that security vendors can't find them. They're using a variety of tricks to do that. The rate of attacks and their sophistication is unlike anything we've seen in the past."

THE EVOLVING THREAT LANDSCAPE

TOM FIELD: Let's talk about the current threat landscape. How do you see today's threats evolving?

TAYLOR ETTEMA: I've been looking at internet and web-based attacks for over 10 years now, and the threat landscape is always evolving. But this time it is different – just the rate of change and the amount of sophistication, particularly in the areas of evasion where adversaries, ever present, ever trying to get into corporate networks by any means necessary, are using a lot of the same attacks we're all familiar with, like credential phishing, malware attacks, web-based attacks, but they're getting ever more adept at hiding those attacks so that security vendors can't find them. They're using a variety of tricks to do that. The rate of attacks and their sophistication is unlike anything we've seen in the past.

FIELD: Why are we seeing this evolution? Is it an oversimplification to say it's the result of accelerated digital transformation?

ETTEMA: We're seeing it because, to some extent, virtually everyone has some amount of network security technology now – web security, email security. The layers are there, and everyone's checking the right boxes. But the reality is much more complex than that. Adversaries know everyone has a web proxy of some sort, or web security. Everyone has email security. So they are building fairly sophisticated ways to evade those technologies. For instance, in the area of web-based attacks, adversaries are putting up victim validation checks in front of their attacks so that when I, as a victim user, go to a phishing page, I see the phishing page. But when a web security vendor crawls that page to find out if it's malicious or not, to add it to their database of malicious web links, they're presented with a blank page or some benign page. That's one of the techniques that adversaries use to hide themselves from security vendors or products.

WHY TRADITIONAL SECURITY SOLUTIONS FAIL

FIELD: Why do traditional security solutions fail to protect against these modern threats?

ETTEMA: On the network security side, once an attacker penetrates a network, one of the key steps in that kill chain is something we call

command-and-control. They'll land on an endpoint within the network, beacon back home and establish that command-and-control channel. Back in the day, every security vendor out there would find these malicious payloads, analyze how their command-and-control, or C2, works and add those C2 traffic patterns to databases or signatures of known C2 patterns. IPS vendors and web security vendors could find these C2 patterns to detect and block them. That was the status quo for the last several, couple dozen years.

What has changed is the proliferation of commercially available red team or penetration test team tools or hack tools, like Cobalt Strike, which is a very pervasive tool. Cobalt Strike and tools like it allow any attacker to create highly and easily customizable C2 profiles, which makes the traffic look like anything they want, and it's very simple to do. These tools democratize fairly sophisticated command-and-control traffic in a way that no IPS or network security product is equipped to defend against. So now, legacy IPS vendors are struggling to keep up with this unknown, custom command-and-control generated by tools like Cobalt Strike, which are marketed as penetration tests or red team tools but are used by virtually every attacker group out there, even at the nation-state level. Why use and expose your own tools when you can just use a commodity off the shelf that does everything you need it to do and more, and makes attribution harder?

On the web security side, I mentioned that attackers are putting up attack gates. Before the phishing page is released to your victim, they're checking: "Is that my intended target? Are they coming from the browser I expect? Are they coming from the geolocation I expect?" Attackers are putting up capture challenges, where you have to click where you see the bicycle in front of the phishing attack so that it's only released to a human. But when someone crawls that website to do automated analysis, which is how the bulk of web security is still done today – believe it or not, most web security products rely predominantly on database lookups of known malicious URLs – they won't see those web attacks.

REQUIREMENTS FOR DEFENSE

FIELD: What types of security capabilities are required today to defend against these threats you've just described?

ETTEMA: One common theme ties all these things together: We cannot rely anymore on the techniques of old, simple pattern-matching, web crawling-based approaches – basic antivirus and IPS techniques. We need to provide sophisticated analysis to see the attacks as they happen and detect and prevent them. For a long time now, we've used a subset of machine learning called deep learning, which is very sophisticated and very big and costly to run, historically. Deep learning is very helpful for security challenges if you can keep it running at low latency, at high performance and yet cost effectively enough to detect and prevent these attacks as they happen. Despite the

"We've found a way to use deep learning technology to detect and prevent advanced, evasive attacks. We keep the deep learning in the cloud, but we have our network security platform doing SASE cloud-delivered network security."

challenges, vendors have used technology like this for several years. It sits in their big clouds doing out-of-band analysis, trying to find the attacks after they happen so that it can then generate protections. But it's too late by that point. The victim has been successfully compromised in the meantime.

THE PALO ALTO NETWORKS APPROACH

FIELD: How do Palo Alto Networks' security subscriptions help defend against the innovative techniques that attackers use today?

ETTEMA: We now have Advanced URL Filtering, which is our flagship web security product. We have Advanced Threat Prevention, which brings inline deep learning to the network security and IPS use case as well. And we've got amazing technology updates to our DNS Security service. All three of these bring deep learning inline to solve some of the hard challenges that I mentioned. We've found a way to use deep learning technology to detect and prevent advanced, evasive attacks. We keep the deep learning in the cloud, where it needs to be for the scale, the compute and the complexity. But we have our network security platform, whether it be on-premises next-generation firewalls or our Prisma Access service up in the cloud, doing SASE cloud-delivered network security. Either form factor can loop in deep learning inline on the network transactions and web sessions that it needs to see in order to fight and prevent today's advanced attacks.

FIELD: How do these services work together to provide what you describe as the industry's most comprehensive security solution?

ETTEMA: If each of these capabilities was operating in a silo, it might be somewhat useful at detecting and preventing what it is seeing, but it misses an opportunity to potentially prevent other attacks down the road or protect other stages of the same attack. But the services talk to each other. For example, if we analyze an unknown malware in our sandbox, detonate it and see that it's C2 traffic to a specific domain or URL, we can add that callback traffic to our web security services, our DNS security services, so that we can see it and prevent it anywhere else in your network, even if the payload wasn't seen.

OUR VISION IS A WORLD WHERE EACH DAY IS SAFER AND MORE SECURE THAN THE ONE BEFORE

Palo Alto Networks, the global cybersecurity leader, continually delivers innovation to enable secure digital transformation—even as the pace of change is accelerating

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io