NSFOCUS

Understanding the Threat Intelligence Ecosystem

Stephen Gates of NSFOCUS on How to Enhance Cybersecurity with Actionable TI

ISMG
INFORMATION SECURITY
MEDIA GROUP

NSFOCUS

Gates is a key research intelligence analyst with NSFOCUS. He has been instrumental in solving the DDoS problem for service providers, hosting providers and enterprises in North America and abroad. He has more than 25 years of computer networking and security experience with an extensive background in the deployment and implementation of next-generation security solutions. He is a recognized subject matter expert on DDoS attack tools and methodologies, including next-generation defense approaches.

Everybody talks about Threat Intelligence (TI) today, but how well are they distinguishing raw data from actionable intelligence? **Stephen Gates of NSFOCUS** discusses cybersecurity and the new threat intelligence ecosystem.

"'Actionable advice' are the two most important words" defining threat intelligence, says Gates, Chief Research Intelligence Analyst at NSFOCUS. Threat intelligence means a lot of things to a lot of people, Gates says, but ultimately, "It's really all about gaining further insight into the threat landscape your organization faces on a daily basis."

In an interview about the threat intelligence ecosystem, Gates discusses:

- How many organizations fail to distinguish actionable TI;
- Why the ecosystem is so critical to cybersecurity;
- How NSFOCUS distinguishes itself in a crowded marketplace.

Defining Threat Intelligence

TOM FIELD: Steve, tell me about NSFOCUS and your specific role there, please.

STEVE GATES: NSFOCUS was founded in the year 2000 and is headquartered in Beijing, China and Silicon Valley, California. We have more than 2,000 global employees and almost 8,000 customers worldwide. We're an active member of the global security community and the world's largest cybersecurity company you've never heard of.

My role at NSFOCUS is to provide commentary. That means blogging and creating content designed to advance NSFOCUS' message to a global scale, making people aware that NSFOCUS exists and about the technologies and solutions we're bringing to the market.

FIELD: Steve, everybody has their own concept of what threat intelligence is. How do you define it?

GATES: I always start off with the explanation from Gartner. According to Gartner, threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.

"Actionable advice" are the two most important words out of that entire paragraph. Threat intel means different things to different people. It could be a data feed, a dashboard, or analyst reports. It could be common vulnerability databases, common weaknesses databases, situational awareness, AV signatures, correlation engines, auto next-gen firewalls, IPS, WAF policy creation. It means a lot of different things to a lot of different people.

It means knowing more about the 4.3 billion IP addresses in the world of IPv4. We have more than 4.3 billion IP addresses and devices, and many of those devices could be sitting behind NAT firewalls.

IPv6, which is coming soon, will have 7.9 times 10 to the 28th power times the address space of IPV4. That is one large number with a lot of zeroes behind it. There are more than 249 million domain names registered globally across all top-level domains as of March 2015, and close to 300 million domains today. There are probably billions and billions of distinct URLs.

There are close to 18 million distinct malware signatures today. And there are a huge number of attack vectors, attack motivations, and attack techniques. It's really all about gaining further insight into the threat landscape your organization faces on a daily basis. That's what threat intelligence is all about.

Leveraging the Value of Threat Intelligence

FIELD: Steve, this could sound like an obvious question, but I think your unique perspective is going to be valuable. The question is: What value does threat intelligence bring to an organization's overall security strategy?

GATES: Threat intel is all about what you do with it. When you sign up for a subscription service, which can be very expensive, what do you do with that information? The questions your audience needs to ask themselves include:

- Do I want to be able to proactively block potential attacks and information leakage?
- How can I gain more context into the security alerts I currently see?
- How can I get more context into the vulnerabilities and exploits that my systems are facing every day?
- How can I get better risk assessment to detect threats and attacks more quickly?

What we're really trying to achieve is better security through faster detection. We know there is an impact associated with the length of time that an attacker has residence inside of a network. Take the Wendy's attack. The attackers remained resident in its network for well over six months, and debit and credit card information was stolen from over 1,000 restaurants. We've got to shorten that window from measure to countermeasure.

Studies have shown that the longer it takes to identify a threat, the greater the damage. Threat intel can help solve some of those problems and also shorten the time from measure to countermeasure. At NSFOCUS, we believe we can get that down to seconds, from the actual infection to detection, and then remediation that generally follows.

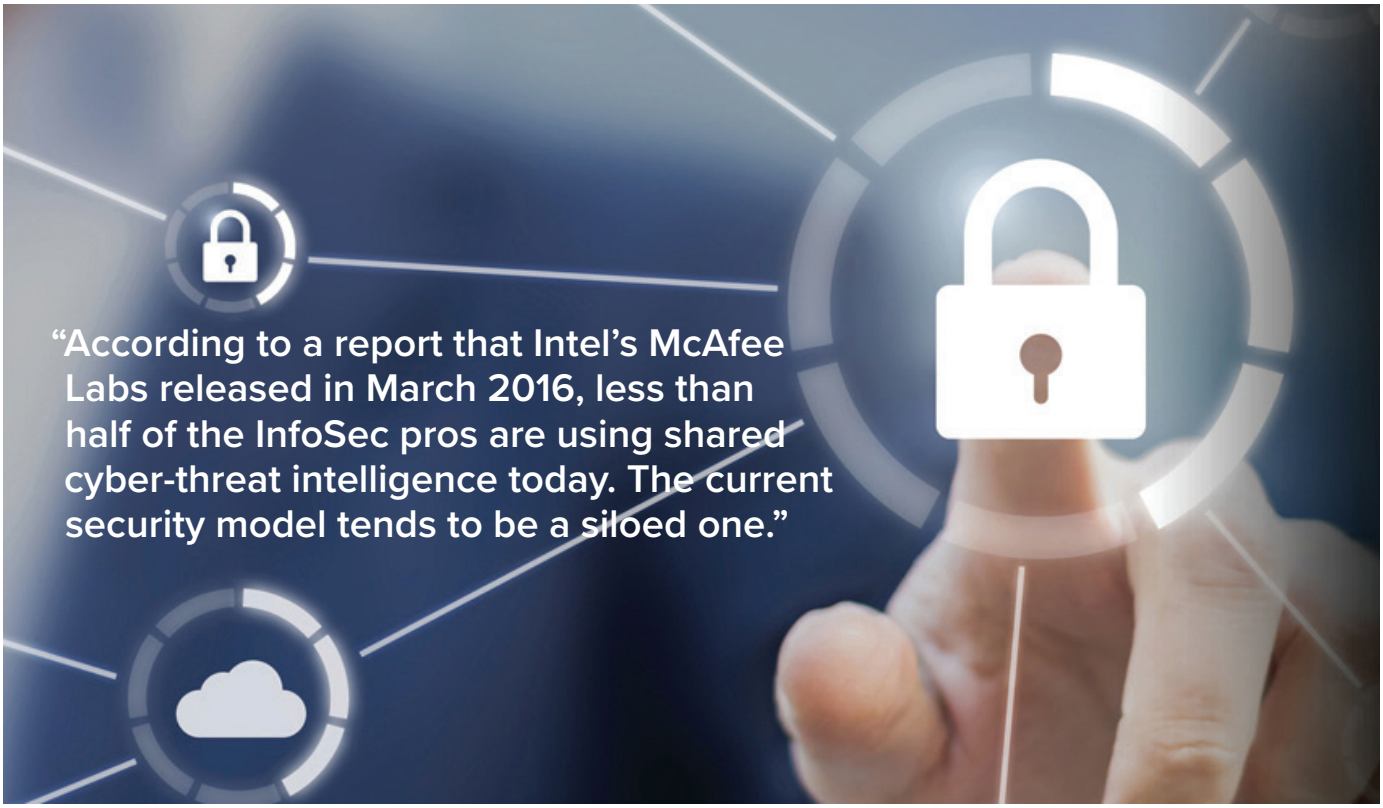
"What we're really trying to achieve is better security through faster detection. We know there is an impact associated with the length of time that an attacker has residence inside of a network."

Why 'Actionable Threat Intelligence' Is Different

FIELD: There's a difference between threat intelligence and actionable threat intelligence. In what ways are people failing to distinguish that difference?

GATES: According to a report that Intel's McAfee Labs released in March 2016, less than half of the InfoSec pros are using shared cyber-threat intelligence today. The current security model tends to be a siloed one. We have firewalls. We have intrusion detection and prevention systems. We have anti-virus. We have anti-DDoS in hardware and software formats. They tend to be static and reactive.

What we're trying to move towards is an intelligent hybrid security model, where all of these technologies are now fed threat intelligence into a security platform. We're talking about something that's extremely adaptive, dynamic and proactive, able to actively block new and emerging threats and reduce OPEX through dynamic and automatic updates to your current security policies. It's all about simplifying these threat-hunting initiatives.



The Threat Intelligence Ecosystem

FIELD: Steve, at the outset, I talked about the threat intelligence ecosystem. What is this ecosystem? Why is it so critical now to cybersecurity?

GATES: The NSFOCUS Threat Intelligence ecosystem allows customers to seamlessly incorporate threat context into their NSFOCUS products, or any third-party products for that matter. This highly curated data primarily comes from NSFOCUS research labs, in conjunction with their technology deployments all over the world. In addition, the data also comes from strategic partnerships with other providers of threat intelligence, enables faster detection of and response to the dangerous IP addresses that are trying to access your infrastructure, as well as any of your users visiting risky domains and URLs. Machines communicate with known command-and-control infrastructures. Malware propagation today is just a huge problem, growing exponentially.

The SANS InfoSec Reading Room Report, *Who’s Using Cyberthreat Intelligence and How* offers some interesting statistics. Twenty-eight percent of the respondents see at least 26 percent better context, accuracy, and/or speed in monitoring and incident handling. Also, 63 percent of respondents say cyber threat intel has improved the visibility into attack methodologies. And 51 percent see faster and more accurate detection or response, and 48 percent cite reduction incidents through early prevention due to threat intel.

As we can see, organizations are gaining the value from threat intel if it’s implemented in an actionable fashion.

Visibility in China: The NSFOCUS Difference

FIELD: Where does NSFOCUS get its threat intelligence, and how does that distinguish your company in what has become a very crowded marketplace?

GATES: First and foremost, NSFOCUS is internationally recognized for our contributions on a global threat intelligence scale. For example, we’re a Microsoft Bug Bounty Award winner for the last four consecutive years. We created a 200-plus node honeypot system across 31 provinces in China. We are a founding member of the Cloud Security Alliance and a regular contributor to the CVE (Common

Vulnerabilities and Exposures) database, having discovered and reported over 40 vulnerabilities just within the last few years.

If you look at today's statistics, up to 40 percent of the world's attacks are estimated to originate from China. And NSFOCUS had a very humble beginning inside of China. We currently have more than 8,000 customers, primarily in the APAC region and primarily inside of mainland China. We have access to all of our customers' networks, organizations that want to opt into our crowdsourcing campaigns where we allow them to participate in our threat intelligence platforms. We collect more than 700 GB of data daily. We have over 700 managed services customers. We have 12,000 networks and over 40,000 systems deployed, and we're monitoring all of those systems across this entire infrastructure. We have an extensive honeypot system. We have partners in curated data. As a matter of fact, we partner with an organization that has attack visibility of 400 million endpoints inside of mainland China.

The real question for your audience: Is there a current blind spot or missing piece in your current threat intel approach? The other question is: Can NSFOCUS feeds fill that blind spot and complete the puzzle? Also, how important is it to have a complete global picture of the threats your organization faces daily? I sense many people listening to this interview will agree they lack visibility into threat intelligence derived from China. This is something NSFOCUS provides.

As a matter of fact, I had an opportunity to participate at Black Hat Conference this year. You see all those vendors out on the expo floor, all trying to differentiate themselves and bring something unique to the market. But NSFOCUS offers threat intelligence from a Chinese perspective, which truly is unique. This is the blind spot everyone has today with regards to their threat Intel, and NSFOCUS can solve that problem.

"What we're trying to move towards is an intelligent, hybrid security model, where all of these technologies are now feeding threat intelligence into a security platform. ... something that's extremely adaptive, dynamic and proactive."

Upcoming Solutions from NSFOCUS

FIELD: Tell me a little bit more about the company. Specifically, what types of strategies and solutions can the marketplace expect to see?

GATES: In the next few months, NSFOCUS' cloud offering will begin to gain market share. We've already implemented our threat intelligence inside of our cloud. This is 1.2 TB cloud with seven different defense centers around the globe. The differentiation we have brought to our cloud strategy will change the way people think about the hybrid security solutions out there today.

Also, NSFOCUS plans to release its next generation IPS and threat analysis technology later this year that will have the competitors taking some serious notice. With up to 20 GB in performance on a single appliance, it will be the fastest solution on the market. Virtualized platforms will be available as well.

In addition, NSFOCUS' web application firewall will be available later this year. This technology will provide the best defenses and the best performance at a price point people will be able to adopt rapidly. Released in both hardware and virtual form factors, the vision of NSFOCUS is to bring all of our technologies, both cloud and on-premise solutions, under our threat intelligence umbrella.

This solution will deliver the world's first intelligent hybrid security solution, all completely integrated under a single pane-of-glass management platform and supporting optional crowdsourcing where users can actually contribute to our global threat intelligence. ■

---

http://www.bankinfosecurity.com/interviews/understanding-threat-intelligence-ecosystem-i-3272

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.

Contact

(800) 944-0401
sales@ismgcorp.com

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.

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismgcorp.com