We keep the record straight by preserving government websites, news articles, historical data, and more. If you find our archive useful, please CHIP IN

INTERNET ARCHIVE WayBackMachine http://www.georgekurtz.com/2012_02_01_archive.html Go
7 captures
26 Jan 2013 - 23 Apr 2021
DEC JAN 26 APR 2012 2013 2015 About this capture

Wednesday, February 22, 2012

CrowdStrike launches in stealth-mode with $26 million Series A round led by Warburg Pincus

As I mentioned in a previous post, I was delighted to announce that I had joined Warburg Pincus, a leading global private equity firm focused on growth investing, as an Executive in Residence. So far my time as an EIR at Warburg has been fantastic. The past few months have exposed me to many new companies and technologies that really got my creative juices flowing and pushed me to get back into the start-up game with Warburg Pincus as my partner.

Today, I am proud to announce the stealth-mode launch of my newest venture that I co-founded with Dmitri Alperovitch (CTO) and Gregg Marston (CFO) – CrowdStrike. CrowdStrike is a security technology company focused on helping enterprises and governments protect their most sensitive intellectual property and national security information. Utilizing Big-Data technologies, CrowdStrike is developing a new and innovative approach to solving today's most demanding cyber-security challenges. CrowdStrike's core mission is to fundamentally change how organizations implement and manage security in their environment.

Why CrowdStrike:

The seemingly daily barrage of disclosures about companies that have had their crown jewels stolen in recent years reinforced a key principle for us – ***these companies don't have a malware problem, they have an adversary problem.*** Many just don't know it. Today's attacks are sophisticated, targeted, and long ranging in scope. Unfortunately, almost every security solution focuses on the tens of thousands of pieces of malware, exploits, and vulnerabilities that are seen in the wild every day. Yet, those are just the interchangeable and, in many cases, disposable tools that the adversaries use to achieve their ultimate objective – theft of intellectual property, trade secrets, and other business proprietary information.

As many of you know the security industry is building "Maginot-line" style of defenses – attempting to prevent all adversaries from getting inside the perimeter of the network or host system. More importantly, a well-financed, trained, and highly determined attacker will always get in. More than likely, they are already in. There is no silver bullet that will stop a determined adversary, so while the security industry attempts to build bigger fences, the enemy is bringing higher ladders to the fight. Moreover, the industry continues to focus on the malware or exploits which is akin to focusing on the gun as opposed to the shooter committing the crime. The person or organization pulling the trigger (or deploying the malware) is the one that you ultimately need to focus on. The type of gun or ammunition they may be using is interesting, but in most cases not strategically relevant.

Based upon investigations we have led, such as Operation Aurora, Night Dragon, and Shady RAT, and knowing the limitations of existing technologies, we are horrified at the amount of IP being stolen and financial damage inflicted every day. It is evident that we are dealing with economic predators who are systematically destroying value in countries around the world. Even worse, we may very well see the enemy engage in destructive and disruptive attacks designed to take down critical infrastructure or modify key processes and data in a covert undetectable fashion.

The Missing Link: Attribution & Raising the Costs to the Adversary

Attribution is the key strategic piece missing from all existing security technologies – providing the answer to the "who?" vs. the "what?" Knowing who is after your IP is critical in determining what assets you want to protect and how. Protecting everything is impossible – you may as well be protecting nothing. However, knowing the enemy is the first step in the process of

About This Blog

This blog was created to connect with other passionate users about all things security. It will also reflect on the start-up world and entrepreneurship.

About Me

George Kurtz

President and CEO CrowdStrike, Former Chief Technology Officer & EVP McAfee, Former CEO of Foundstone. Co-Author:Hacking Exposed

View my complete profile

Blog Archive

▼ 2012 (5)
► September (1)
► August (1)
► May (1)
► April (1)
▼ February (1)
CrowdStrike launches in stealth-mode with $26 mill...
► 2011 (3)

Lastest Twitter Updates

Join the conversation

Follow by Email

Email address... Submit

Linkedin Profile

View my profile on LinkedIn

Amazon

GoSecure, Inc.
Exhibit 2013
CrowdStrike v. GoSecure
IPR2025-00070

We keep the record straight by preserving government websites, news articles, historical data, and more. If you find our archive useful, please CHIP IN

INTERNET ARCHIVE WayBackMachine http://www.georgekurtz.com/2012_02_01_archive.html Go DEC JAN 26 APR 2012 2013 2015 About this capture

7 captures
26 Jan 2013 - 23 Apr 2021

the answer to the "who?" vs. the "what?" Knowing who is after your IP is critical in determining what assets you want to protect and how. Protecting everything is impossible – you may as well be protecting nothing. However, knowing the enemy is the first step in the process of determining the priority of allocation of scarce resources to defend the key assets and tailoring your response to the Tactics, Techniques and Procedures (TTPs) of the adversary. Knowing their capabilities, objectives, and the way they go about executing on them is the missing piece of the puzzle in today's defensive security technologies. The key to success is raising adversary's costs to exceed the value of the data they may be trying to exfiltrate and the only way to accomplish that is by forcing them to change the way they conduct the human-led parts of their intrusions, such as reconnaissance, lateral movement, identification of valuable assets, and exfiltration. Other parts of the operation, such as vulnerability weaponization, malware delivery, and command and control can be mass-produced and changed at will with little cost. However, attackers are creatures of habit and while they are fast to change their weapons, they are slow to change their methods. **By identifying the adversary and revealing their unique TTPs (i.e. modus operandi), we can hit them where it counts – at the human-dependent and not easily scalable parts of their operations.**

The CrowdStrike Mission:

As the President and CEO of CrowdStrike, one of the most exciting aspects of this new venture for me is assembling a "dream team" of security visionaries to address this important mission and challenge. Our team is comprised of people who are "big thinkers" that have the technical prowess to execute and carry out our mission goals without the encumbrances that face legacy security solutions. Our team of visionaries are the rebels who believe the current state of security is fundamentally broken and want to do something about it. More importantly, these are the patriots who are tired of seeing our intellectual property and competitive advantage wiped away under the thinly veiled cover of an Internet address. The recent stories surrounding Nortel provide a shinning example of how the adversaries can embed themselves into a multi-national organization for the better part of a decade without detection while systematically accessing their most coveted intellectual property. If we sit back idly and do nothing about these types of attacks, we certainly face a crisis of epic proportions and economic consequences that we have yet to fully comprehend. CrowdStrike does not accept the status quo, and we intend to do something about it. If you share our passion and vision about this crisis, and believe you have what it takes to join our fight then please send an email to mission@crowdstrike.com. We are looking for kick ass coders, consultants, and experts who like us have been fighting and responding to nation-state targeted intrusions.

I will leave you with one final thought. The ancient Chinese military strategist Sun Tzu in his teachings emphasized the need to "know your enemy". For if "you know your enemy and know yourself," he wrote, "you need not fear the result of a hundred battles." Isn't it time we apply these simple time honored lessons in the cyber security battlefield of the twenty-first century?

If you would like to keep up with the latest news on CrowdStrike please follow us on Twitter @CrowdStrike.

If you are attending the RSA conference next week, you can look for us at the following events we are speaking at:

Monday February 27: America's Growth Capital 8th Annual Information Security Conference

10:15-11:00 am Mobile Security The Changing Threat and Remediation Landscape (panel with George Kurtz)
3:30-4:15 pm Combating State-Sponsored Adversaries (panel with Dmitri Alperovitch)

Wednesday February 29: RSA Conference

8:00-9:10 am Cyber Battlefield: The Future of Conflict
10:40-11:30 am Hacking Exposed: Mobile RAT Edition

Posted by George Kurtz at 3:44 PM 4 comments:

amazon
SHOP. CONNECT. ENJOY.

Newer Posts Home Older Posts

Subscribe to: Posts (Atom)

We keep the record straight by preserving government websites, news articles, historical data, and more. If you find our archive useful, please CHIP IN

INTERNET ARCHIVE WayBackMachine http://www.georgekurtz.com/2012_02_01_archive.html Go DEC JAN 26 APR 2012 2013 2015 About this capture
7 captures
26 Jan 2013 - 23 Apr 2021

adversary's costs to exceed the value of the data they may be trying to exfiltrate and the only way to accomplish that is by forcing them to change the way they conduct the human-led parts of their intrusions, such as reconnaissance, lateral movement, identification of valuable assets, and exfiltration. Other parts of the operation, such as vulnerability weaponization, malware delivery, and command and control can be mass-produced and changed at will with little cost. However, attackers are creatures of habit and while they are fast to change their weapons, they are slow to change their methods. **By identifying the adversary and revealing their unique TTPs (i.e. modus operandi), we can hit them where it counts – at the human-dependent and not easily scalable parts of their operations.**

The CrowdStrike Mission:

As the President and CEO of CrowdStrike, one of the most exciting aspects of this new venture for me is assembling a "dream team" of security visionaries to address this important mission and challenge. Our team is comprised of people who are "big thinkers" that have the technical prowess to execute and carry out our mission goals without the encumbrances that face legacy security solutions. Our team of visionaries are the rebels who believe the current state of security is fundamentally broken and want to do something about it. More importantly, these are the patriots who are tired of seeing our intellectual property and competitive advantage wiped away under the thinly veiled cover of an Internet address. The recent stories surrounding Nortel provide a shinning example of how the adversaries can embed themselves into a multi-national organization for the better part of a decade without detection while systematically accessing their most coveted intellectual property. If we sit back idly and do nothing about these types of attacks, we certainly face a crisis of epic proportions and economic consequences that we have yet to fully comprehend. CrowdStrike does not accept the status quo, and we intend to do something about it. If you share our passion and vision about this crisis, and believe you have what it takes to join our fight then please send an email to mission@crowdstrike.com. We are looking for kick ass coders, consultants, and experts who like us have been fighting and responding to nation-state targeted intrusions.

I will leave you with one final thought. The ancient Chinese military strategist Sun Tzu in his teachings emphasized the need to "know your enemy". For if "you know your enemy and know yourself," he wrote, "you need not fear the result of a hundred battles." Isn't it time we apply these simple time honored lessons in the cyber security battlefield of the twenty-first century?

If you would like to keep up with the latest news on CrowdStrike please follow us on Twitter @CrowdStrike.

If you are attending the RSA conference next week, you can look for us at the following events we are speaking at:

Monday February 27: America's Growth Capital 8th Annual Information Security Conference

10:15-11:00 am Mobile Security The Changing Threat and Remediation Landscape (panel with George Kurtz)
3:30-4:15 pm Combating State-Sponsored Adversaries (panel with Dmitri Alperovitch)

Wednesday February 29: RSA Conference

8:00-9:10 am Cyber Battlefield: The Future of Conflict
10:40-11:30 am Hacking Exposed: Mobile RAT Edition

Posted by George Kurtz at 3:44 PM 4 comments:

Newer Posts Home Older Posts

Subscribe to: Posts (Atom)

Awesome Inc. template. Powered by Blogger.