SearchSecurity

GRANDEDUC - FOTOLIA

TIP

How studying the black hat community can help enterprises

White hat hackers often assimilate themselves into the black hat community to track the latest threats. Discover how this behavior actually benefits the enterprise with David Geer.

David Geer, Geer Communications

Editor's note: *This is part two of a series on the limitations of traditional threat intelligence and the value that white hat hackers can offer enterprises. Part one looked at what threat intelligence often doesn't tell you about new and emerging threats.*

Well-connected white hats can tell you what tools and threats black hat hackers are currently developing and the vulnerabilities they are chasing. This allows them to then purchase and use these tools to penetration test your network for vulnerabilities, enabling flaws to be fixed before new attacks go public.

White hats get this data by accessing closed, secret forums on the dark web -- a place where webmasters can block search engines from indexing their sites and where encrypted networks are used to hide the site's existence.

White hat hackers often pose as black hats to participate and engage in the black hat community and earn the confidence of members within closed hacker forums. Black hat members must recommend users before they can become members themselves, said Ryan Olson, contributing author of *Cyber Fraud: Tactics, Techniques and Procedure* and vice president of threat intelligence at Palo Alto Networks.

Once inside the black hat community forums, white hats can observe the content of criminal hacker conversations, what they are working on and which tools are considered best-selling. Within these forums, white hats can also find links to additional markets.

"There you can often purchase hacked, stolen credentials; access to compromised machines inside specific organizations; and access to dumps -- data from breaches," said Francisco Donoso, a veteran security expert and head of managed security services architecture at Kudelski Security. "You may want to be able to search for people who are selling access to stolen accounts or compromised machines at large enterprise organizations [and white hats can search for you.]"

Closed underground forums post the latest tools and threats, such as new remote access tools for controlling enterprise computers from a distance. Popular tools attract the most interest because developers share a lot of updated versions and continually add new features, said Olson. Posting in forums is one way that a white hat can recognize a tool that is more likely to slip past security products and become a more significant threat to the enterprise.

> **The dark web is full of useful information for the concerned enterprise.**

s full of useful information for the concerned enterprise. White hats can use it to tell you what the black hat community is cooking up in their secret labs, such as weaponized AI, said Rene Kolga, CISSP and a 10-year veteran cybersecurity expert.

At Black Hat USA 2017, the presentation "Bot vs. Bot for Evading Machine Learning Malware Detection" demonstrated how malware coders use the same machine learning algorithms that security vendors do to enable malware to avoid detection using machine learning-enabled security products. Some of these algorithms and tools can be used by threat actors for nefarious purposes.

"Hackers use machine learning tools [such as machine learning as a service] provided by major cloud providers like Amazon, Microsoft and Google like anyone else," Kolga said. "Hackers procure antimalware solutions powered by machine learning to test their new malware."

White hats face certain risks

White hats must maintain their relationships and image in the black hat community if they want to have continued access to data.

"If you're a white hat doing that under multiple personas in different languages [such as Chinese or Russian] on multiple forums on a regular basis, it is an intelligence process where you are managing sources, maintaining relationships and keeping them fruitful so you can get the information you need when you need it," said Olson.

White hats who undertake these endeavors face risks, as they must walk a fine line when engaging in the forums so people trust them -- meaning they may have to buy some tools and give feedback, which some would consider a questionable activity, according to Olson. Infosec professionals and their organizations should use white hats that know and stay on the right side of that line so the company doesn't find itself on the wrong side.

The solution is to contract or hire a white hat who maintains these kinds of relationships and access within the black hat community so that you can stay a step ahead of criminal hackers rather than play catch up after disaster strikes.

This was last published in June 2018

Related Resources

Evolve your Endpoint Security Strategy Past Antivirus and into the Cloud
–SearchSecurity.com

Five Tips to Improve a Threat and Vulnerability Management Program
–SearchSecurity.com

Demystifying the myths of public cloud computing
–ComputerWeekly.com

Towards an Autonomous Vehicle Enabled Society: Cyber Attacks and Countermeasures
–ComputerWeekly.com

Dig Deeper on Threats and vulnerabilities

white hat hacker

By: Andrew Froehlich

black hat hacker

By: Katie Terrell Hanna

GovTech launches vulnerability rewards programme

By: Aaron Tan

By: Aaron Tan

hacker

By: Wesley Chai

ETWORKING CIO ENTERPRISE DESKTOP CLOUD COMPUTING COMPUTER WEEKLY

SearchNetworking

Next-gen network management difficult without AIOps

Complicated networks mean complicated network management. AIOps can help manage next-generation networks by monitoring, adding ...

Troubleshoot name resolution on Windows, Linux and macOS

Network administrators can troubleshoot name resolution using a variety of methods, including ping, nslookup and PowerShell ...

About Us Editorial Ethics Policy Meet The Editors Contact Us Videos Photo Stories

Definitions Guides Advertisers Business Partners Media Kit Corporate Site

Contributors CPE and CISSP Training Reprints Events E-Products

Privacy Policy

Do Not Sell My Personal Info