To InformationWeek

Advertise With Us
About Us
Contact Us
Welcome Guest
Login to your account
Register

SECTIONS

- Home
- News & Commentary
- Authors
- Slideshows
- Video
- Reports
- White Papers
- Events
- Black Hat
- Attacks/Breaches
- App Sec
- Cloud
- Endpoint
- Mobile
- Perimeter
- Risk
- Operations
- Analytics
- Vulns/Threats

- Login to your account
- Register
- About Us
- Contact Us
- Advertise with Us

Search Dark Reading

- Facebook
- Twitter
- LinkedIn
- Google+
- RSS

InformationWeek DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

Search Dark Reading

Follow DR:

Home
News & Commentary
Authors
Slideshows
Video
Radio
Reports
White Papers
Events
Black Hat
SECURITY JOBS

Analytics
Attacks / Breaches
App Sec
Careers & People
Cloud
Endpoint
IoT
Mobile
Operations
Perimeter
Risk
Threat Intelligence
Vulns / Threats

Attacks/Breaches

3/30/2016
10:30 AM

Gunter Ollmann
Commentary

Connect
Directly

0 comments
Comment

50%50%

Like 38 Tweet Share 111 G+1 7

Machine Learning In Security: Good & Bad News About Signatures

Why security teams that rely solely on signature-based detection are overwhelmed by a high number of alerts.

First in a series of two articles about the history of signature-based detections, and how the methodology has evolved to identify different types of cybersecurity threats.

Used in the context of an outdated and manually intensive technology focused on older classes of threats, there' s little wonder why vendors would seek to distance the legacy term "signature" from their advanced detection technology. Vendors haven' t necessarily been deceptive in the labeling of their latest generation of techniques; it' s often just easier to create a new label for something than to fully explain the context and evolution of what preceded it.

Over the years, signature-based systems have changed and advanced, but the core concepts still lie at the heart of all modern detection systems – and will continue to be integral for the foreseeable future. To understand what a "signature system" is in reality, we need to understand the evolution of the detection path as directed and discovered by human intervention.

One-dimensional signatures: Blacklists and whitelists are examples of one-dimensional signature systems. They are found throughout security and exist in practically all detection and protection technologies. They are by far the fastest and most efficient way of categorizing a data artifact (e.g. a domain name, IP address, user-agent, MD5 hashes, etc.). As a Boolean operation, what you' re looking for is either on the list or it is not.

Two-dimensional signatures: Classic regular-expression functions and string matching are examples of two-dimensional signature systems. They are the fundamental building blocks of anti-malware, intrusion detection, and data leakage detection systems. In malware, they are often used to search a binary file for known strings which help to label the type of threat it represents. Two-dimensional signatures came to the fore as a means of detecting network-based threats within the content-level of traffic – easily capable of identifying previously known exploits and host enumeration techniques.

Data leakage prevention (DLP) is a more recent security technology that relies heavily upon two-dimensional signatures. Messages and file attachments are often scanned for specific strings (e.g. serial numbers, passwords, etc.) or construction formats (e.g. social security numbers of the format nnn-nn-nnnn with a regular expression of ^\d{3}-\d{2}-\d{4}$).

Multidimensional signatures: Security vendors developed a hybrid system as the threat spectrum grew and attackers found new ways to obfuscate the elements of their attacks that were most exposed to one-dimensional and two-dimensional signatures. Instead of triggering on a single signature, a multi-dimensional signature was created. In both sandboxing and network behavioral monitoring, certain actions and activities are labeled as either suspicious or bad.

When a threshold of good or bad activities is reached, the threat is classified and labeled. For example, a suspicious file is executed within a virtual environment. The file attempts to write to the Windows registry (neither good nor bad), add a file to the Windows startup path (suspicious), disable Windows updates (bad), read from the user’s contacts list (neither good nor bad), and then send email to every address listed in the contacts list (bad).

Together, all of these individual actions (i.e. signatures) are combined and tallied and a decision is made that the suspicious file is in fact malicious and most likely a spambot.

Signature systems all share the same characteristic of being able to promptly identify and label a threat. As signature systems have evolved, they have become capable of detecting and classifying a broader range of threats. In modern detection and prevention systems, a combination of different signature systems are used together so they can most accurately label a known threat, but this also has the problem of generating a high number of alerts that can overwhelm a team that solely relies on signature-based detection for security purposes.

Historically, the linear progression and sophistication of signature-based detection systems have been dependent upon human signature writers. For each new threat, a unique signature or signature artifact is created by a skilled engineer or security researcher. This pairing between signature and its human creator means that as the number of threats have increased, so too have the number of skilled personnel needed to develop and support the signatures that detect them. For obvious reasons, this is not a scalable business proposition – for neither the vendor or customer.

New developments in machine learning – in particular supervised and unsupervised learning algorithms – are now being applied to information security and are paving the way to a new class of signature systems capable of economically scaling to the threat.

Next in the series: *Machine Learning In Security: Seeing the Nth Dimension in Signatures*

Related Content:

- 3 Flavors of Machine Learning: Who, What & Where
- Machine Learning Is Cybersecurity's Latest Pipe Dream
- Machine Learning: Perception Problem? Maybe. Pipe Dream?

Gunter Ollmann is chief security officer at Vectra. He has nearly 30 years of information security experience in an array of cyber security consulting and research roles. Before joining Vectra, Günter was CTO of Domain Services at NCC Group, where he drove strategy ... View Full Bio

Comment | Email This | Print | RSS

State of UC Research: Future Adopters to Reap Benefits via Cloud

More White Papers

Reports

[InformationWeek & Dark Reading Report] 2015 Strategic Security Survey Results

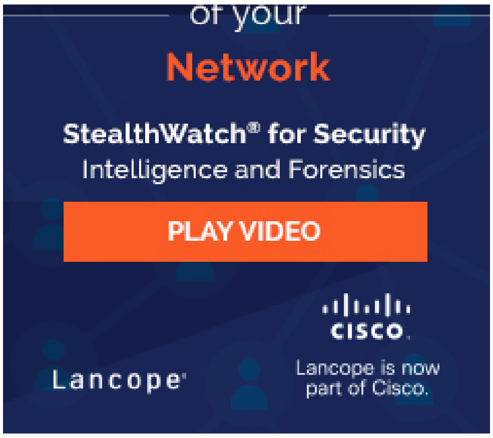
Research: 2014 Strategic Security Survey

More Reports

Comments

Newest First | Oldest First | Threaded View

Be the first to post a comment regarding this story.


of your
Network
StealthWatch® for Security
Intelligence and Forensics
PLAY VIDEO
cisco
Lancope
Lancope is now part of Cisco.

Subscribe to Newsletters

Live Events

Webinars

UBM Tech

More UBM Tech Live Events

Virtualization & Data Center Track at Interop Las Vegas

Attend the Collaboration Track at Interop Las Vegas

Come to Interop Las Vegas, May 2 - 6, 2016

White Papers

3-D Secure: The Force for CNP Fraud Prevention Awakens

Features & Benefits with NetSupport DNA

Negotiating with Cybercriminals

Breaking Through WAN Performance Barriers and Deploying the Right Tools

Centralizing Business Communications: Remove Complexity and Gain Cost Savings and Scalability

More White Papers

Video

Cartoon

All Videos

Good morning, 555-00-6742, makes 73,000 a year, has 3 credit cards.
Hello owes 107,000 on a mortgage, with a family history of heart disease.
klossner

Latest Comment: Although obviously poking fun at things, this cartoon is probaly not far from the truth. We just won't be staring at screens - we'll have our ...

Cartoon Archive

Current Issue

UBM

InformationWeek Tech Digest

Understanding and Managing the Mobile Security Threat

Mobile devices are increasing IT security risk. Is your enterprise ready? >>

By Ericka Chickowski

Also Inside

Zero Trust: Now a Critical Foundation For Securing Mobile >>

FAQ: Here's What You Need to Know About the Apple, FBI Dispute >>

Powered by InformationWeek DARKReading

Understanding & Managing the Mobile Security Threat

Mobile devices are increasing IT security risk. Is your enterprise ready?

Download This Issue!

Back Issues | Must Reads

Flash Poll

What's missing from your incident response plan? (Pick all that apply.)

☐ Access to activity logs

☐ An up-to-date network diagram

☐ Blueprint for public disclosure

☐ Hostname-IP address maps

☐ IR fire drills before the event

□ IR fire drills before the event

□ Plan for finding malicious files after the breach

□ We don't have an incident response plan

□ Other (Please explain in the comments)

Submit

All Polls

Rub shoulders with the nation's most innovative and imaginative CIOs
Ken Spangler
SVP & CIO, FedEx Ground
& FedEx Freight Systems
InformationWeek ELITE 100 CONFERENCE
REGISTER NOW ›

Slideshows

Cybercrime: A Black Market Price List From The Dark Web

0 comments | Read | Post a Comment

6 Hot Cybersecurity Startups: MACH37's Spring Class Of 2016 0 comments

What The Feds Said At RSA 1

More Slideshows

Twitter Feed

Tony Cleal @tony_cleal

NIST Cybersecurity Framework Adoption Hampered By Costs, Survey Finds darkreading.com/attacks-breach… via @DarkReading

30m

Syed Hassan Mussana Retweeted

Tenable Security @TenableSecurity

High cost of implementation keeping many from adopting NIST Cybersecurity Framework ow.ly/105SKz via @DarkReading

14h

Francis Gorman Retweeted

ZeroDayJobs @zerodayjobs

How Facebook Bakes Security Into Corporate Culture buff.ly/1LJ3FpT via @DarkReading

7h

Bug Report

Enterprise Vulnerabilities
From DHS/US-CERT's National Vulnerability Database

CVE-2013-7445
Published: 2015-10-15
The Direct Rendering Manager (DRM) subsystem in the Linux kernel through 4.x mishandles requests for Graphics Execution Manager (GEM) objects, which allows context-dependent attackers to cause a denial of service (memory consumption) via an application that processes graphics data, as demonstrated b...

CVE-2015-4948
Published: 2015-10-15
netstat in IBM AIX 5.3, 6.1, and 7.1 and VIOS 2.2.x, when a fibre channel adapter is used, allows local users to gain privileges via unspecified vectors.

CVE-2015-5660
Published: 2015-10-15
Cross-site request forgery (CSRF) vulnerability in eXtplorer before 2.1.8 allows remote attackers to hijack the authentication of arbitrary users for requests that execute PHP code.

CVE-2015-6003
Published: 2015-10-15
Directory traversal vulnerability in QNAP QTS before 4.1.4 build 0910 and 4.2.x before 4.2.0 RC2 build 0910, when AFP is enabled, allows remote attackers to read or write to arbitrary files by leveraging access to an OS X (1) user or (2) guest account.

CVE-2015-6333
Published: 2015-10-15
Cisco Application Policy Infrastructure Controller (APIC) 1.1j allows local users to gain privileges via vectors involving addition of an SSH key, aka Bug ID CSCuw46076.

Dark Reading Radio

Archived Dark Reading Radio

When Will Passwords Finally Die?

Join Dark Reading Executive Editor Kelly Jackson Higgins as she talks to authentication experts to find out what the future holds.

UPCOMING!
Wednesday, April 13, 1pm EDT
Advancing Your Security Career

FULL SCHEDULE | ARCHIVED SHOWS

InformationWeek DARKReading

About Us
Contact Us
Customer Support
Sitemap
Reprints

Twitter
Facebook
LinkedIn
Google+
RSS

UBM

Technology Portfolio

Black Hat
Cloud Connect
Dark Reading
Enterprise Connect

Fusion
GDC
GTEC
Gamasutra

HDI
ICMI
InformationWeek
Interop

Network Computing
No Jitter
Tower & Small Cell Summit

COMMUNITIES SERVED

Enterprise IT
Enterprise Communications
Game Development
Information Security
IT Services & Support

WORKING WITH US

Advertising Contacts
Event Calendar
Tech Marketing
Solutions
Contact Us
Licensing