(http://sqrrl.com)

Target. Hunt. Disrupt.

BLOG (HTTP://BLOG.SQRRL.COM/) REQUEST A DEMO (HTTP://SQRRL.COM/CALL-TO-ACTION/DEMO/) TEST DRIVE VM (HTTP://INFO.SQRRL.COM/TRIAL-SOFTWARE-VM-1) CONTACT US (HTTP://SQRRL.COM/COMPANY/CONTACT-US/)
(HTTP://SQRRL.COM/COMPANY/BLOG/)

HOME (HTTP://SQRRL.COM/)

PRODUCT (HTTP://SQRRL.COM/PRODUCT/SQRRL-ENTERPRISE)

SOLUTIONS (HTTP://SQRRL.COM/SOLUTIONS/USE-CASES/)

PARTNERS (HTTP://SQRRL.COM/PARTNERS/)

SERVICES (HTTP://SQRRL.COM/SERVICES/SQRRL-ENTERPRISE-SUPPORT/)

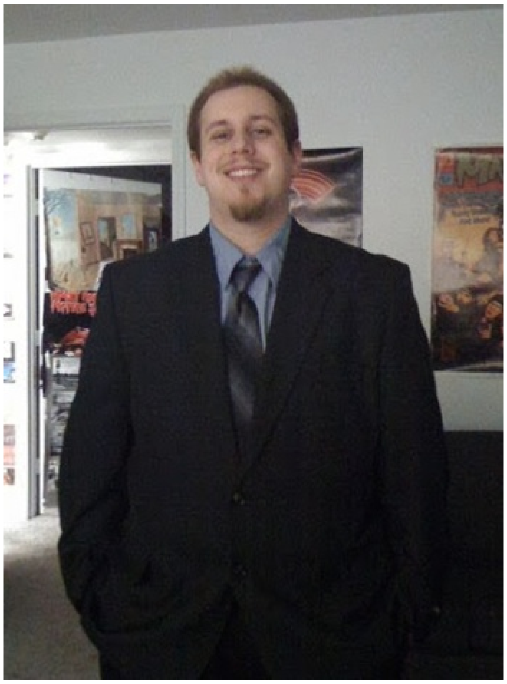
RESOURCES (HTTP://SQRRL.COM/RESOURCES/ASK-AN-EXPERT/)

COMPANY (HTTP://SQRRL.COM/COMPANY/OVERVIEW/)

SQRRL BLOG

Mar 29, 2017 8:00:00 AM

Threat Hunter Profile - Ryan Nolette (http://blog.sqrrl.com/threat-hunter-profile-ryan-nolette)



Name: Ryan Nolette

Organization: Sqrrl

Years hunting: 7

Favorite datasets: Process execution, process parentage, registry key modification/creation, IDS/IPS logs, Bro, firewall logs

Favorite hunting techniques: Daily dynamic list creation, OODA looping, data traversal analysis

Favorite tools: Bro, Snort, Suricata, Sqrrl, volatility, nmap, Wireshark, REMnux, SIFT, PFsense, malzilla

Who are you?

Jokes aside, I am currently a Security Technologist at Sqrrl driving the research and development of new detection and analytic features and products for the Sqrrl platform. I joined Sqrrl from Carbon Black where I held a variety of roles including threat research, incident response consulting and ultimately, leading the company's security operations efforts. With over a decade in the infosec field, I have been on the product and operations side of companies such as Crossbeam Systems, SecureWorks and Fidelity Investments. I have been an active speaker and writer on threat hunting and endpoint security in the last few years, and with a little digging, you can find some of my work (like here (https://goo.gl/1ADAUx), here (https://www.youtube.com/watch?v=dlvvoXitrII), and here (https://github.com/sonofagl1tch)).

Why do you hunt and what is your experience hunting?

I have been threat hunting since ~2010 when it was called many things, but the term threat hunting was not yet coined. My mantra was always proactive detections minimize impact and cost to my organization. I also believe in automating anything I have to do more than twice which is what led me to start creating SIEM correlations and scripts for hunting so I could teach junior analysts to do the same things I was doing.

I started my first Hunting team out of necessity. I was working an IR, forensically focused) and supporting a customer who needed more than what their Sysadmin (operations based) could detect. I ended up using some techniques I discovered in previous engagements to find Zeus on multiple systems in the customer environment based on the persistence mechanisms that it used at that time. Eventually, this evolved from a one-off exercise to the development of a Hunting strategy/methodology that could be integrated into a SOC and repeated. I now try to teach what I have learned throughout my career to help others protect themselves.

How do you define Threat Hunting?

I am going to steal Alan Orlikoski (http://blog.sqrrl.com/threat-hunter-profile-alan-orlikoski)'s answer and say “Hunting is the process of looking for interesting events that are not defined as malicious by existing automated tools. It uses the knowledge, tools, data, and experience that exists within an organization to determine if events are associated with an attacker or innocuous.” I couldn't have said it better myself.

What projects and organizations are you involved with?

I am currently the treasurer of the HTICA New England chapter (https://htcia.org/chapter/new-england/). This organization aims to aid collaboration between local and federal law enforcement, military and government organizations, and the private sector. I have also spoken at or worked with SANS, Bsides Boston, Bsides North Carolina, Infragard NE Chapter, ISACA/IIA, ISC2, ACSC, and multiple colleges.

Which of the hunts you've carried out was the most interesting or challenging?

This one started as a single thread based on kernel panic on a Jenkins server and unwinded to showcase a major enterprise breach. To simplify and shorten the story I am going to just write a numbered list in order of what I found then the process the attacker used for compromise.

- Findings:
  - Kernel panic on Jenkins server used for creating software builds of internal products
  - Firewall logs to support data exfiltration
  - NAS access logs to show data collection
  - System access logs to show intruder activity on entire build environment
  - Endpoint artifacts to show persistence mechanisms, backdoors, and data exfiltration attempts from multiple systems

Building the Story of the Attack

1. Attacker attempts to phish company
   - Sends to ~30 hand picked employees
   - No on clicks and almost all emails are reported to SecOps. Go user training!
2. Scanning of external facing company network

   - No footholds found willing to accept inbound connects and accepted and exploits/access attempts made by the attackers.
   - Attacker discovery of PBX system
3. Attacker find old firmware for PBX system and reverse engineers a 0-day that is still usable
4. Attacker users 0-day to get into PBX system and then starts recon
5. Attacker finds that PBX is not segment off from the rest of the network as shown on company network diagrams
   - I attribute this to process break down and fatigue from fast pace required of the administration teams.
6. Attacker then moves laterally to NAS
   - Has no UAC implemented. Basically a big bucket that anyone can read or write to.
   - *insert tears here*
7. Attacker starts to exfiltrate data from NAS through the PBX and out to their servers
   - No network alerts fired because nothing was setup to detect large file transfers from the PBX systems.
8. Attacker discovers employee VM that hasn't been patched since Reagan was president.
9. Attacker owns VM and uses it to continue recon on the internal network.
   - Because the VM is NAT'd and there are not security controls in place to view this traffic separately, it looks like it is coming from the user's system directly when seen in firewall and router logs.
10. Attacker finds Jenkins system from employee's VM
    - Attacker is able to SSH into Jenkins without a password due to the user have an SSH key without passwords on it and Jenkins is setup to allow passwordless SSH.
11. Attacker SSH's into Jenkins
    - Gold mine found. SSH keys for passwordless SSH access to all build slaves, source code repos, and probably the last clean pair of underwear in the build are there
    - Attacker goes shopping and takes everything they can.
    - Exfiltration attempts fail directly from Jenkins because it is blocked from outbound network access by the firewall.
    - Attacker is required to transfer files from Jenkins to compromised VM out to their servers
12. Attacker attempts to install keyloggers, backdoors, and persistence on Jenkins but accidentally injects a backdoor into the wrong process and causes the system to kernel panic and reboot.
13. Employees request a Linux admin look into the issues with the server and the admin find binaries that are strange to him and escalates the ticket to SecOps for helps finding root cause of the issue.
14. SecOps confirms existence of backdoor, declares and incident, and starts the process of finding what happened.
15. SecOps comes up blank because no automated detection tools find anything and the team is lacking expertise on the OS in question.
16. I get called in to see what I can find
    - I pulled network logs, system logs, endpoint agent logs, off the bat
    - While waiting for them to be collected I look into the kernel panic and find that the panic message states that binary "malware123" (yes i made that name up) was attempting to access the running jenkins process (I can't get more specific due to NDA) and showed the full path to the binary.
    - I pull a copy of the binary and toss it into REmux. I find out it is a simple ELF binary and decode it to find a few shared libraries and the holy grail of hardcoded IP addresses and hostnames used for the C&C server.
17. I use my new found artifacts to search through all the newly correlated data to find 20+ systems reaching out to these known addresses.
18. I expand scope of the hunt to go through these systems to find more artifacts and rinse and repeat my searches. In all 36 systems were owned, 16 user systems, 12 servers, 5 appliances (PBX systems) and 3 network devices.

Whew. And that was one of the more exciting hunts I've done.

What hunting techniques, tools, and datasets do you use most frequently?

The Sqrrl Hunting Loop is a great model to use when creating hunting activities as it addresses the methodology and feedback loop inherent in every hunting activity. I reference the OODA loop whenever I talk about defensive and reactive security, but it also applies to proactive security like threat hunting and should be adopted by more hunters.

I commonly will take techniques, tools, or processes I find in blogs, webinars, or presentations and apply them in my environment in an attempt to add context to things I am already findings and to find things I have not even thought to look for yet.

In general, I enjoy digging into data traversing the intranet to internet boundaries as well as internal segment boundaries in a micro-segmented network. This is a great way to find things trying to hide in plain sight or at least find bad user configurations that need to be fixed before they become bigger issues.

I also enjoy creating daily dynamic lists to track source machine names for all failed login attempts using service accounts and other various common tasks that will find high-risk users and violators of policy. Sometimes the results from a threat hunt are less than glamorous and are more about good security hygiene internally.

What value do you actively see come out of your hunting activities?

Practice makes perfect and finding things is only 1 half of threat hunting. Being able to confidently state that nothing was found because there is nothing there is the other half, and that comes later in the process. Regardless of the outcome of a threat hunt I perform, my goal is to find context until i give confidently answer the question I am asking.

What types of friendly intelligence are most useful for a hunter to have in an investigation?

- Network topology
- Data classification
- Critical resources
- Additional security controls and visibility tools I can use to add context to data and convert it into actionable intelligence

What general advice do you have for new Threat Hunters?

READ! Subscribe to blogs and webinars as much as possible. Everyone is trying to figure out solutions to different problems and the same problems. Use their experience to guide you and learn as much as possible. You are eventually going to reference one of those techniques or tools to accomplish your job.

What hunting procedure would you recommend for a new to Threat Hunter?

Start poking at your data now. Look for obvious things like BitTorrent traffic so you can see what data looks like. Now add more sources. Do they give you more context about what the user was doing? Why or why not? Rinse and repeat for other types of traffic and events. If you aren't constantly poking at your data, how will you know what is normal and what isn't when the time comes to do it under pressure?

"I use Sqrrl to find those dark places in my environment, poke it with a stick, and see what crawls out."
-Ryan Nolette

What parts of a hunt could you see as being most successfully automated or assisted by a machine?

The automation aspect is a key to the threat hunting cycle because there is always is way too much data and not enough people. Humans are great at the creative analytics and design and develop new methods to hunt. Once they have been developed, it is important to automate those pieces, so you can scale.

What would you like to see Threat Hunting develop into across the industry in the future?

I would like to see threat hunting become a regular security audit that organizations are required to perform on a regular basis to maintain compliance. Currently, threat hunting is considered as a one-time project, when it should be a continuously process similar to making sure you are updating and patching regularly.

(//cta-service-cms2.hubspot.com/ctas/v2/public/cs/c/?cta_guid=06445338-cea9-4e28-8169-0c9ca908bd31&placement_guid=07112381-cd1d-421b-b145-0bb2c47f7ada&portal_id=305377&redirect_url=APefjpHSP0NR44ZJg2ZgFZ_S-oWq8TFXWeikBoFShvHRE7T0Dng3pU77b4BmRCg_r19EDZp44mZHW-P_XQxQAButvUjAOFRAKQisnxmdwZibmfNVpwyzpiwBpbnv3Rry0P--g_KP-_eEXkbHadJkr6z8PW-684wJqA&hsutk=&canon=http%3A%2F%2Fblog.sqrrl.com%2Fthreat-hunter-profile-ryan-nolette&pageId=4975334034)

Check out our full Hunter Profile series (http://blog.sqrrl.com/topic/hunter-profile) for different takes, tips and tricks on threat hunting from the experts!

Topics: Cyber Hunting (http://blog.sqrrl.com/topic/cyber-hunting), Threat Hunting (http://blog.sqrrl.com/topic/threat-hunting), Threat Detection (http://blog.sqrrl.com/topic/threat-detection), Hunter Profile (http://blog.sqrrl.com/topic/hunter-profile)

(http://www.facebook.com/share.php?u=http%3A%2F%2Fblog.sqrrl.com%2Fthreat-hunter-profile-ryan-nolette%3Futm_medium%3Dsocial%26utm_source%3Dfacebook) (http://www.linkedin.com/shareArticle?mini=true&url=http%3A%2F%2Fblog.sqrrl.com%2Fthreat-hunter-profile-ryan-nolette%3Futm_medium%3Dsocial%26utm_source%3Dlinkedin) (https://twitter.com/intent/tweet?original_referer=http%3A%2F%2Fblog.sqrrl.com%2Fthreat-hunter-profile-ryan-nolette%3Futm_medium%3Dsocial%26utm_source%3Dtwitter&url=http%3A%2F%2Fblog.sqrrl.com%2Fthreat-hunter-profile-ryan-nolette%3Futm_medium%3Dsocial%26utm_source%3Dtwitter&source=tweetbutton&text=Threat+Hunter+Profile+-+Ryan+Nolette) (https://plus.google.com/share?url=http%3A%2F%2Fblog.sqrrl.com%2Fthreat-hunter-profile-ryan-nolette%3Futm_medium%3Dsocial%26utm_source%3Dgoogle_plus) (https://mail.google.com/mail/?view=cm&fs=1&tf=1&to=&su=Check%20out%20http%3A%2F%2Fblog.sqrrl.com%2Fthreat-hunter-profile-ryan-nolette%3Futm_medium%3Dsocial%26utm_source%3Demail%20&body=Check%20out%20http%3A%2F%2Fblog.sqrrl.com%2Fthreat-hunter-profile-ryan-nolette%3Futm_medium%3Dsocial%26utm_source%3Demail)

Company

Job Title

Email*

Phone Number

Comment*

□

Subscribe to follow-up comments for this post

Type the text
(http://www.google.comPrivacy & Terms)

SUBMIT COMMENT

(https://twitter.com/SqrrlData) (https://www.facebook.com/SqrrlData) (https://www.linkedin.com/company/sqrrl) (https://plus.google.com/116795302724746825954/posts)

Subscribe to Email Updates

Email*

SUBSCRIBE

Recent

Threat Hunter Profile - Ryan Nolette (http://blog.sqrrl.com/threat-hunter-profile-ryan-nolette)
The Nuts and Bolts of Detecting DNS Tunneling (http://blog.sqrrl.com/the-nuts-and-bolts-of-detecting-dns-tunneling)
What is Threat Hunting in Cybersecurity Defense (http://blog.sqrrl.com/what-is-threat-hunting-in-cybersecurity-defense)
Top 4 Takeaways from RSA 2017 (http://blog.sqrrl.com/top-4-takeaways-from-rsa-2017)
Threat Hunter Profile - Deirdre Morrison (http://blog.sqrrl.com/threat-hunter-profile-deirdre-morrison)

Archive

March 2017 (2) (http://blog.sqrrl.com/archive/2017/03)
February 2017 (3) (http://blog.sqrrl.com/archive/2017/02)
January 2017 (4) (http://blog.sqrrl.com/archive/2017/01)

December 2016 (3) (http://blog.sqrrl.com/archive/2016/12)
November 2016 (4) (http://blog.sqrrl.com/archive/2016/11)
October 2016 (7) (http://blog.sqrrl.com/archive/2016/10)
September 2016 (3) (http://blog.sqrrl.com/archive/2016/09)
August 2016 (3) (http://blog.sqrrl.com/archive/2016/08)
July 2016 (1) (http://blog.sqrrl.com/archive/2016/07)
June 2016 (2) (http://blog.sqrrl.com/archive/2016/06)
May 2016 (4) (http://blog.sqrrl.com/archive/2016/05)
April 2016 (4) (http://blog.sqrrl.com/archive/2016/04)
March 2016 (2) (http://blog.sqrrl.com/archive/2016/03)
February 2016 (2) (http://blog.sqrrl.com/archive/2016/02)
January 2016 (2) (http://blog.sqrrl.com/archive/2016/01)
December 2015 (1) (http://blog.sqrrl.com/archive/2015/12)
November 2015 (3) (http://blog.sqrrl.com/archive/2015/11)
October 2015 (3) (http://blog.sqrrl.com/archive/2015/10)
September 2015 (5) (http://blog.sqrrl.com/archive/2015/09)
August 2015 (5) (http://blog.sqrrl.com/archive/2015/08)
July 2015 (5) (http://blog.sqrrl.com/archive/2015/07)
June 2015 (4) (http://blog.sqrrl.com/archive/2015/06)
May 2015 (1) (http://blog.sqrrl.com/archive/2015/05)
April 2015 (1) (http://blog.sqrrl.com/archive/2015/04)
March 2015 (4) (http://blog.sqrrl.com/archive/2015/03)
February 2015 (1) (http://blog.sqrrl.com/archive/2015/02)
January 2015 (1) (http://blog.sqrrl.com/archive/2015/01)
December 2014 (1) (http://blog.sqrrl.com/archive/2014/12)
November 2014 (1) (http://blog.sqrrl.com/archive/2014/11)
October 2014 (2) (http://blog.sqrrl.com/archive/2014/10)
August 2014 (2) (http://blog.sqrrl.com/archive/2014/08)
July 2014 (1) (http://blog.sqrrl.com/archive/2014/07)
June 2014 (2) (http://blog.sqrrl.com/archive/2014/06)
May 2014 (3) (http://blog.sqrrl.com/archive/2014/05)
April 2014 (1) (http://blog.sqrrl.com/archive/2014/04)
February 2014 (3) (http://blog.sqrrl.com/archive/2014/02)
January 2014 (4) (http://blog.sqrrl.com/archive/2014/01)
December 2013 (3) (http://blog.sqrrl.com/archive/2013/12)
November 2013 (2) (http://blog.sqrrl.com/archive/2013/11)
October 2013 (2) (http://blog.sqrrl.com/archive/2013/10)
September 2013 (2) (http://blog.sqrrl.com/archive/2013/09)
August 2013 (4) (http://blog.sqrrl.com/archive/2013/08)
July 2013 (3) (http://blog.sqrrl.com/archive/2013/07)
June 2013 (5) (http://blog.sqrrl.com/archive/2013/06)
May 2013 (6) (http://blog.sqrrl.com/archive/2013/05)
April 2013 (1) (http://blog.sqrrl.com/archive/2013/04)
March 2013 (4) (http://blog.sqrrl.com/archive/2013/03)
February 2013 (2) (http://blog.sqrrl.com/archive/2013/02)
January 2013 (2) (http://blog.sqrrl.com/archive/2013/01)
December 2012 (3) (http://blog.sqrrl.com/archive/2012/12)
November 2012 (5) (http://blog.sqrrl.com/archive/2012/11)
October 2012 (9) (http://blog.sqrrl.com/archive/2012/10)
September 2012 (1) (http://blog.sqrrl.com/archive/2012/09)
August 2012 (15) (http://blog.sqrrl.com/archive/2012/08)
July 2012 (1) (http://blog.sqrrl.com/archive/2012/07)

(https://twitter.com/SqrrlData) (http://www.facebook.com/SqrrlData) (https://plus.google.com/116795302724746825954/posts) (https://www.linkedin.com/company/2649984)

PRODUCT (HTTP://SQRRL.COM/PRODUCT/SQRRL-ENTERPRISE/)
Sqrrl Enterprise (http://sqrrl.com/product/sqrrl-enterprise/)
Use Cases (http://sqrrl.com/product/use-cases/)
Test Drive VM (http://info.sqrrl.com/trial-software-vm-1)
Technology (http://sqrrl.com/product/architecture/)
PARTNERS (HTTP://SQRRL.COM/PARTNERS/)
Technology (http://sqrrl.com/partners/)
Service (http://sqrrl.com/partners/)