NETWORKWORLD

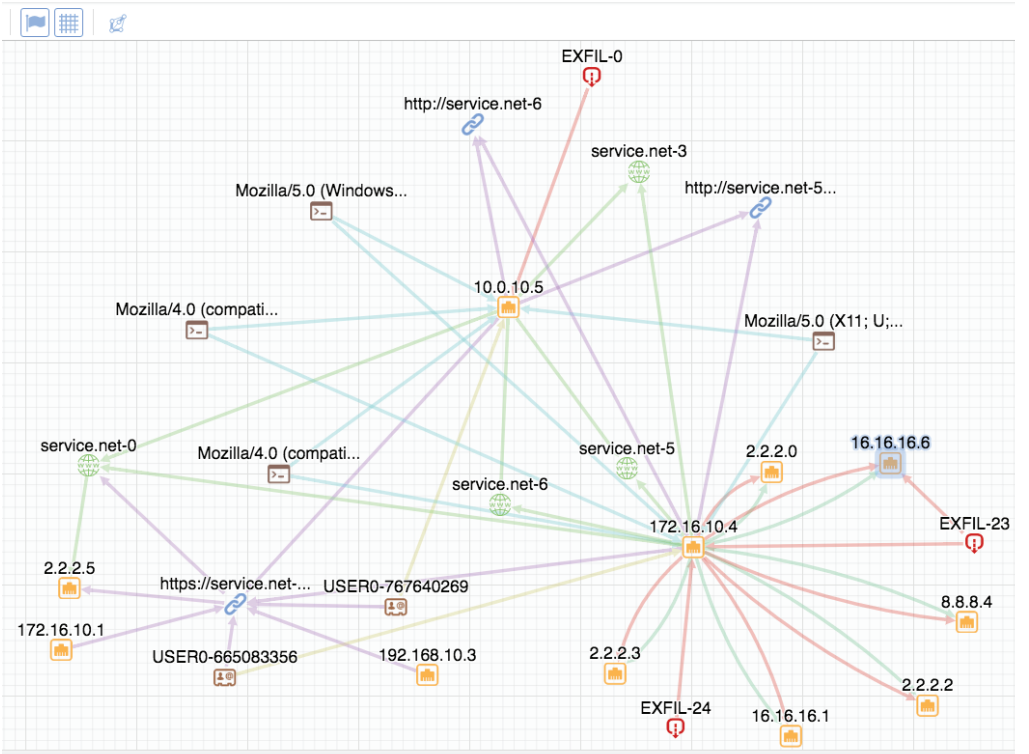
SECURING THE ENTERPRISE

SOLUTION REVIEW

Sqrrl's Threat Hunting Platform

For this review, we tested the threat hunting system from Sqrrl. The platform was tested in a large demo environment seeded with realistic APTs which had bypassed perimeter defenses and were hiding somewhere within the network of virtualized clients and servers. We also snuck active threats past perimeter defenses to see how this threat hunting platform detected, caught and killed the current breed of apex predators of the threat landscape.

The Sqrrl Threat Hunting Platform is a great tool to aid those hunting hidden threats inside their network. It works for users with any skill level, but more experienced analysts will be able to create better theories about attacks and thus likely have more successful hunts.



dst_port	duration	flags	flags_ack	flags_fin	flags_psh	flags_rst	flags_syn	flags_urg	packets	proto	proto_num	src_ip
56238	5	ASFP	true	true	true	false	true	false	10	TCP	6	10.0.0.77
56238	5	ASFP	true	true	true	false	true	false	10	TCP	6	10.0.0.71
56238	5	ASFP	true	true	true	false	true	false	10	TCP	6	10.0.0.71

Sqrrl allows security pros to hunt down advanced persistent threats (APT)

> "It's critical to note that the behaviors which bubble up to the Sqrrl dashboard are not ones that have triggered a SIEM alert."

Let the hunt begin

At the beginning of every day, security analysts are greeted with an overall control panel showing various indicators and suspicious behaviors along with their relative severity. Sqrrl needs about seven days examining user behavior before it can accurately predict the suspicious behavior component, and its machine learning ability makes it even more accurate over time.

Anything over the threshold of potentially malicious behavior set by the network's active security programs is handled by security personnel however they normally would do that. What is left are the odd little things that may, or may not, be an indicator of compromise which has slipped through the cracks.

Hunters can then use their expertise to investigate behaviors like beaconing, lateral movement, data staging, unusual usage patterns and exfiltration to create a hypothesis and potentially uncover a breach. It's possible that hunters can also verify valid activities and clear them from further consideration.

Taking down the threat

Since we knew that most APTs rely on privilege elevation as part of their pattern, we launched an investigation, or hunt, based on a single odd event captured by Sqrrl where an administrator logged into a system labeled C586. The strange thing was that the admin had never touched that system before, but since they logged on using valid credentials the first time they tried, no alerts were triggered. Sqrrl flagged the behavior, and thus we began our investigation.

The great thing about Sqrrl is that everything is displayed visually. We didn't have to pore through the 85 pages of related log files, although they were available if we wanted, to find out what other systems had connected or were somehow involved with C586. We sent in a query from the drop-down menu and discovered a chain going back through four other systems with lateral movement ties to the one under investigation.

From there, we looked at beaconing behavior and discovered that the next system in the chain had beaconed out at some point over the previous month. Because beaconing behavior is one way that APTs reach back to their hosts, this was suspicious even though the IP was not one indicated as dangerous by threat intelligence feeds, and thus had not triggered any alarms.

Pushing our hunch, we searched for that IP address and were surprised to discover that two other systems in the same chain had also beaconed out to the same location. Now the picture was becoming more clear.

It also seemed like the fourth system in the chain, which had several denied access attempts recorded, was not actually part of the attack though it had connected with others that were. The failed access attempts were either the legitimate mistakes of a user forgetting their password, or perhaps deliberate camouflage from the attackers attempting to trigger an alarm to get security personnel looking in the wrong place.

Back to the three systems with beaconing behavior. We queried and found a rogue PHP process active on all three. Looking over time, it was clear that each system beaconed out and used that process only long enough to capture a new system before going dark. The attack chain finally stopped after it accessed C586, but didn't install anything on it and did no beaconing from there.

A little while later, the administrator logged into C586 successfully even though they had never done so before. But using Sqrrl, we were able to discover why, and had a very good idea that those credentials were compromised, even though C586 was totally clean and triggered no alarms.

A successful hunt completed

With a successful hunt completed, we could generate a report so that the network could be protected. The administrator's compromised credentials could be rescinded as well as the login passwords for the compromised users. The IP of the beacon could be blocked and the PHP expunged so that the attackers will have wasted all that time only to be stopped short of their actual goal. And their tactics and techniques could be fed back into both Sqrrl and the network SIEM to catch them if they tried again using the same method.

AT A GLANCE

"Sqrrl's a great tool to aid those hunting hidden threats inside their network."

NETWORKWORLD

Product	The Sqrrl Threat Hunting Platform is a great tool to aid those hunting hidden threats inside their network. It works for users with any skill level, but more experienced analysts will be able to create better theories about attacks and thus likely have more successful hunts.
Price	Pricing for Sqrrl is based on the number of hunters who need to use the system and the amount of internal traffic data that needs to be analyzed. A system with a single hunter on a modest sized network would start at $25,000.
Packaging	It is normally installed as software but can be run in a virtualized or even a cloud environment. The installation takes no more than a couple of hours for most deployments. We became fairly proficient hunters and were able to track down leads and uncover hidden threats after only a few hours of instruction.
Key Focus	Sqrrl's focused on helping security analysts hunt down Advanced Persistent Threats (APT) that slip past even the most cutting-edge security defenses.