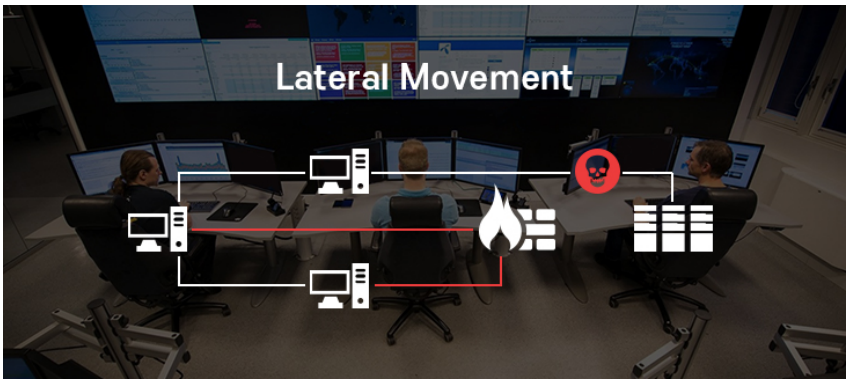
UNDERSTANDING LATERAL MOVEMENT

(/blog/)



(/the-hunters-den-lateral-movement-part-1/)

August 1, 2017 by Ryan Nolette ()

UNDERSTANDING LATERAL MOVEMENT

The Hunter's Den (https://sqrrl.com/topic/how-tos/) blog series aims to go beyond framework and theory and dig into practical tips and techniques for threat hunting. In our previous post, we examined the practical ways to hunt for C2 activity

Browse by Topic

Threat Hunting

Subscribe to Blog

Email Address

SUBSCRIBE

Featured Posts

The Nuts and Bolts of Detecting DNS Tunneling

By Sqrrl Team

(/the-nuts-and-bolts-of-detecting-dns-tunneling/)

(https://sqrrl.com/the-hunters-den-command-and-control/). In this series of posts, we will take a look at how to hunt for lateral movement activity.

Lateral Movement is a critical step in the process of carrying out an attack on a network. It is a category broad enough that it has its own kill chain step (https://attack.mitre.org/w/images/f/f7/ATTaCK_Matrix_Notional.png). Although it is a broad tactic, these posts will survey a specific method that might be carried out by an adversary.

Before we go into detection techniques, let's start by building a foundation of knowledge on Lateral movement. The definition of Lateral movement that I am using is a "term encompassing techniques and tools that enable an attacker to access and/or control systems within your environment."

Something commonly overlooked about lateral movement is that this activity is not the end goal of an attacker, but is instead just a piece of the attack and is often a requirement or dependency of the attacker to achieve their ultimate goal.

The ability to remotely execute scripts or code can be a cornerstone of an attack, but adversaries also attempt to reduce their footprint in environments by abusing legitimate credentials combined with native network and OS functionality to remotely access systems.

Scoping Attacks By Following Attacker Breadcrumbs
By Chris Sanders
(/scoping-attacks-by-following-attacker-breadcrumbs/)

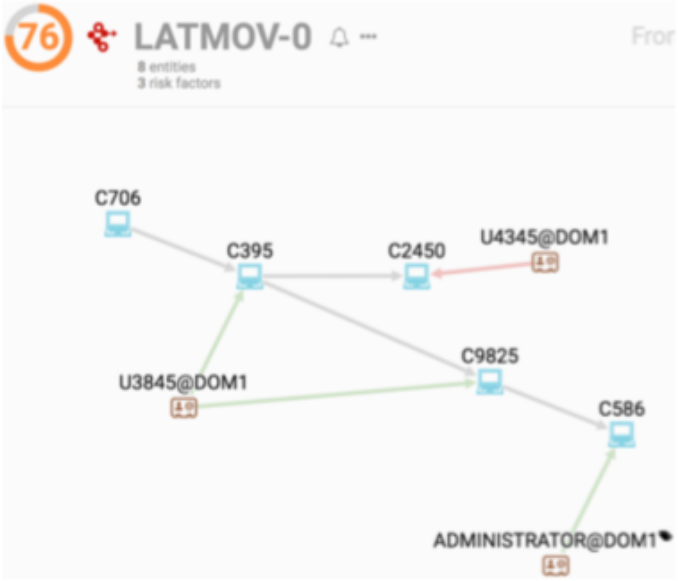
The Hunter's Den: Command and Control
By Josh Liburdi
(/the-hunters-den-command-and-control/)

A Framework for Cyber Threat Hunting Part 1: The Pyramid of Pain
By Sqrrl Team
(/a-framework-for-cyber-threat-hunting-part-1-the-pyramid-of-pain/)

A Framework for Cyber Threat Hunting Part 2: Advanced Persistent Defense
By Sqrrl Team
(/a-framework-for-cyber-threat-hunting-part-2-advanced-persistent-defense/)

Threat Hunting for Command Line Process Execution
By Chris Sanders
(/threat-hunting-for-command-line-process-execution/)

Resources



(https://sqrrl.com/media/1-1.png)

Example of Lateral Movement Activity in Sqrrl

Breaking down the attack further, there are dozens of methods (https://attack.mitre.org/wiki/Lateral_Movement)to achieve lateral movement in an environment. Because of this, the attacker has a wide variety of tricks at their disposal. A few of the most common techniques I have seen in the wild are:

Pass the hash (PTH):

A method of authenticating as a user without having access to the user's cleartext password.

Remote Services:

Where an adversary may use valid credentials to log into a service specifically designed to accept remote connections, such as PsExec, RDP, telnet, SSH, or VNC.

Taint Shared Content:

Content stored on network drives may be tainted by adding applications, scripts, or exploits to otherwise legitimate files.

To demonstrate a typical scenario, we'll look at an example where the attacker will attempt to move from the patient 0 compromised system to gather the company's financial records. Next, the attacker discovers that they cannot directly access the files from the infected host. They then attempt to move laterally to another system they can see on the network. When this system also does not have access to the data the attacker wants, the attacker will attempt to move laterally again and again until finally finding a system with the access they want.

SANS 2017 Threat Hunting Survey
(http://info.sqrrl.com/sans-2017-threat-hunting-report)

Watch Overview

(https://www.youtube.com/watch?v=Vl_zLBc4KQM&t&width=640&h

00:00 00:21

Example of Lateral Movement Activity

HIGH-LEVEL TTP OVERVIEW

We can take the previous scenario and dissect it into stages.

First, we had the initial infection, this occurred by any ordinary means, phishing email, exploit kit, whatever.

Next, we have the compromise stage. This phase differs from the infection stage because we are defining compromise as the attacker has direct access to the system where the infection is defined as automated malware infecting the system. To expand on that, infection is something like getting a trojan on your computer, but compromise does not occur until the malware opens up a connection on the system for an attacker to get direct CLI access to the system.

The third stage is reconnaissance which contains the attacker collecting data about the system they are on and what other systems the attacker can see from the compromised host.

The next stage is credential theft. This stage is vital for the attacker because, without credentials, their ability to move laterally will be extremely limited. Credential theft comes in many forms, and we will dig into that in a bit.

Lastly, comes the actual lateral movement stage where the attacker combines the information they have gathered with the credentials they have gathered and attempt to authenticate to other systems in the environment. These three stages of recon, credential theft, and lateral movement, will be repeated on every system the attacker successfully authenticates.

Tune in next week for the next blog in this series that will show the attack from the attacker side!

And as always, remember my motto, Flag it, Tag it, and Bag it.

(https://sqrrl.com/why-do-you-need-a-hunt-team-the-answer-may-surprise-you/)

July 19, 2017 by David Bianco ()

WHY DO YOU NEED A HUNT TEAM? THE ANSWER MAY SURPRISE YOU! (HTTPS://SQRRL.COM/WHY-DO-YOU-NEED-A-HUNT-TEAM-THE-ANSWER-MAY-SURPRISE-YOU/)

You've probably heard this a million times now: "You need a hunt team". This is true, as far as it goes, but **why**? For most people, the initial answer is probably something close to this: "So we can find bad guys on our network". Again, this is true, but would it surprise you learn that finding the bad guys is probably the least important reason to have a hunt team?

READ MORE
(https://sqrrl.com/why-do-you-need-a-hunt-team-the-answer-may-surprise-you/)

Next Post


(https://twitter.com/SqrrlData)


(https://www.facebook.com/SqrrlData)


(https://plus.google.com/116795302724746825954/posts)


(https://www.linkedin.com/company/sqrrl)


(http://www.youtube.com/user/sqrrldata)

SQRRL NEWSLETTER

Subscribe to our mailing list

Email

SUBMIT

Twitter Feed

@ (http://www.twitter.com/) 17 Aug
Sqrrl's landmark 2.8 release introduces powerful new **#threathunting (https://twitter.com/search?q=%23threathunting&src=hash)** tools like hunter-defined analytics: **https://t.co/h2MP3H9EAf (https://t.co/h2MP3H9EAf)**

@ (http://www.twitter.com/) 17 Aug
Sqrrl 2.8 is out! Check out the new features here: **https://t.co/F3kuNPQTKU (https://t.co/F3kuNPQTKU)**

FOLLOW US ON TWITTER (https://twitter.com/SqrrlData)

PRODUCT (/PRODUCT/SQRRL-ENTERPRISE)
Sqrrl Enterprise (Https://Sqrrl.com/Product/Sqrrl-Enterprise/)
Technology (Https://Sqrrl.com/Product/Architecture/)
Architecture (Https://Sqrrl.com/Product/Architecture/)
Behavior Graph (Https://Sqrrl.com/Product/Behavior-Graph/)
User And Entity Behavior Analytics (Https://Sqrrl.com/Product/User-And-Entity-Behavior-Analytics-Ueba/)
Test Drive VM (Http://Info.sqrrl.com/Trial-Software-Vm-1)

SOLUTIONS (/SOLUTIONS/USE-CASES/)
Use Cases (Https://Sqrrl.com/Solutions/Use-Cases/)
Cyber Threat Hunting (Https://Sqrrl.com/Solutions/Cyber-Threat-Hunting/)
Cyber Incident Investigation (Https://Sqrrl.com/Solutions/Cyber-Incident-Response-And-Investigation/)

PARTNERS (HTTPS://SQRRL.COM/SERVICES/SQRRL-PARTNER-PROGRAM/)
Threat Hunting Ecosystem (Https://Sqrrl.com/The-Sqrrl-Partner-Program/)
Technology (/Partners/Technology)
Sales (/Partners/Sales)

SERVICES (/SERVICES/SQRRL-ENTERPRISE-SUPPORT/)
Sqrrl Enterprise Support (Https://Sqrrl.com/Services/Sqrrl-Enterprise-Support/)

RESOURCES (/RESOURCES/)
Datasheets (/Resources/#Datasheet)
EBooks (/Resources/#Ebook)
Quick Reads (/Resources/#Quick-Read)
Reports (/Resources/#Report)
Videos (/Resources/#Video)
Webinars (/Resources/#Webinar)
Whitepapers (/Resources/#Whitepaper)

COMPANY (/COMPANY/OVERVIEW/)
Overview (Https://Sqrrl.com/Compa
Team (/Company/Team/Manag
Advisors (Https://Sqrrl.com/Compa
Blog (Http://Blog.sqrrl.com)
News Room (Https://Sqrrl.com/Compa
Careers (Https://Sqrrl.com/Compa
Contact Us (Https://Sqrrl.com/Compa

Terms (https://sqrrl.com/terms/)