Rapid7 Quarterly Threat Report: 2017 Q2

Intent, Capability, Opportunity, and the Threat Landscape

By Rebekah Brown, Threat Intelligence Lead, Rapid7, Inc.
Bob Rudis, Chief Security Data Scientist, Rapid7, Inc.
Jon Hart, Senior Security Researcher, Rapid7, Inc.
Dustin Myers, Threat Intelligence Researcher, Rapid7, Inc.
Vasudha Shivamoggi, Data Scientist, Rapid7, Inc.
Philip Thomsen, Data Science Intern, Rapid7, Inc.

August 2, 2017

CONTENTS

Introduction

We had three goals in mind when composing this second edition of the Rapid7 Threat Report. First and foremost, we wanted to—again—provide as clear a picture as possible of the threat landscape organizations faced during the second quarter of 2017. To this end, we've included composite and industry-level views of threat events across many industries.

These threat events do not happen in a vacuum; the second quarter of 2017 was chock full of large-scale attacks with varying degrees of impact that touched almost every organization in some way, shape, or form. For our second goal, we combed through our event and research

data to paint a clearer picture of what happened in Q2 to help you iron out any wrinkles in your incident response programs.

Finally, as we examined the events of the past quarter, we've highlighted key takeaways that are applicable across organizations of every size, shape, and locale. We hope you find the report to be an informative and useful companion as you continue to develop your own detection and response programs.

What Is a Threat?

We throw the term "threat" around a lot, and so it is important to define exactly what it is we mean. When there is an adversary with the intent, capability, and opportunity, a **threat** exists. When there are two or more of these elements present (e.g. an intent and a capability), we call it an **impending threat**, because there is just one missing piece before it becomes a true threat. When there is just one (e.g. an opportunity in the form of a software vulnerability), we call it a **potential threat**. There is the potential for it to turn into a true threat, although there are additional components that need to come to fruition before it has a real impact to most organizations.

Q2 2017 Trends

The second quarter of 2017 kept us on our toes from the first day to the last. Nation-state-level exploits, surprise patches for end-of-life systems, and the newly coined "ransomworm" attacks kept defenders from knowing which way was up for most of the quarter. Some of the trends we captured seem rather obvious, like how patching reduces your risk, even from sophisticated attacks. Unfortunately, other lessons learned were not as self-evident.

LESSONS LEARNED

Lesson #1: One person's meat is another one's poison.

One of the industry-wide lessons from Q2 can be summarized as "importance is in the eye of the beholder." In mid-April of 2017, the Shadow Brokers dumped a cache[1] they claimed belonged to the NSA, and an assortment of sophisticated network exploitation tools was

[1] https://community.rapid7.com/community/infosec/blog/2017/04/18/the-shadow-brokers-leaked-exploits-faq

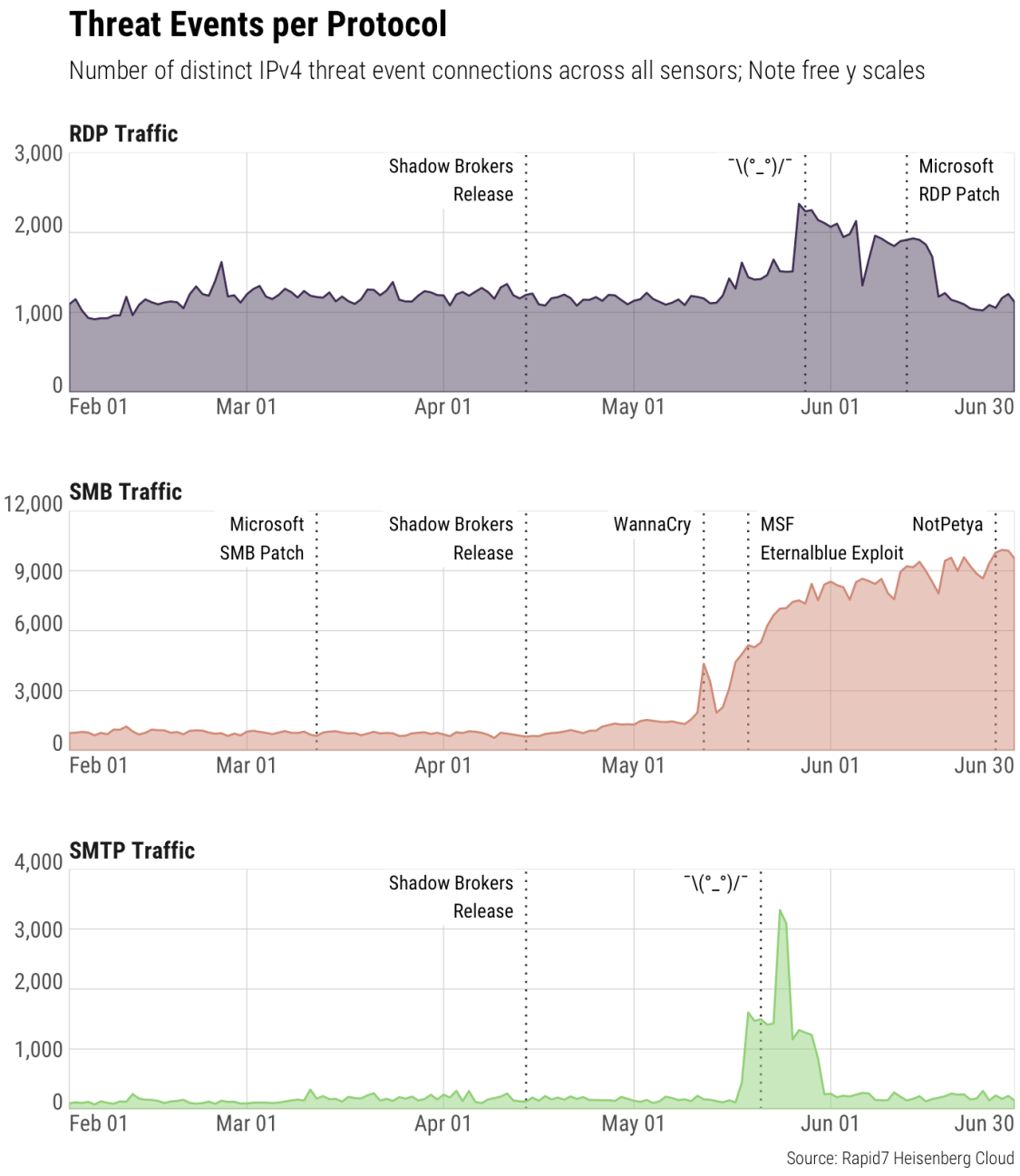
instantly available for anyone to reverse engineer and use. For a brief moment in time, many researchers felt like kids in a candy store. It quickly became apparent that the exploits were antiques and had all been patched, or were for ancient systems. Suddenly, what we thought was a candy store was actually more of a tofu stand, and kids rarely go gaga over tofu. So we (as defenders) moved on. Unfortunately, we were the only ones. Attackers did not move on; they realized that even though we thought we were safe against these non-zero day, unexciting attacks, we were not.

As seen in Figure 1, SMB traffic to our Project Heisenberg honeypots gradually increased following the Shadow Broker's exploit leak mid-April. However, the sharpest spike came in mid-May after attackers paired the leaked exploit with a ransomware variant in an attack known as WannaCry[2]. Since then, SMB traffic has steadily increased. New attacks, including NotPetya[3], continue to appear, despite the fact that these attacks target a vulnerability from which we thought all were safe.

[2] https://community.rapid7.com/community/infosec/blog/2017/05/12/wanna-decryptor-wncry-ransomware-explained

[3] Initial reports used a variety of names for this particular attack, and we're settling in "NotPetya," since it is not only "not Petya," but it's also pretty clearly not ransomware, but merely a disguised data wiper.

Figure 1: Threat Events per Protocol



After the Shadow Brokers dump, we had a fully developed capability**,** and when systems remained unpatched, then there was an opportunity; all that remained to become a true threat was an adversary with the intent, which very quickly manifested itself in more ways than one. The capability—and to some degree, the opportunity—still exist, so it is just a matter of time before a new threat manifests.

The EternalBlue[4] exploit that targeted SMB is not the only one that could be used by attackers. Several other exploits in the batch target mail services, some target IIS web servers, and others target Remote Desktop Protocol (RDP). Many of the vulnerabilities are older, but that doesn't mean that attackers can't, or won't, find a way to take advantage of them; plenty of targets that are still out there make it worth their time and effort, as likely cataloged by Figure 1. After all, the internet is chock full of legacy services[5].

In fact, we saw a sharp, and potentially alarming, spike in RDP traffic at the end of May, shortly after reports[6] that a repurposed version of the leaked RDP exploit, EsteemAudit, was being sold on underground criminal forums. Traffic levels have since returned to normal and a special patch was released by Microsoft[7], which only impacts end-of-life systems. There was another spike in SMTP traffic shortly after that, and while we cannot say with certainty that it is related to any of the leaked email-focused exploits, port 25 exposure is another area that defenders should keep an eye on to ensure there aren't any unidentified opportunities for attackers to compromise systems.

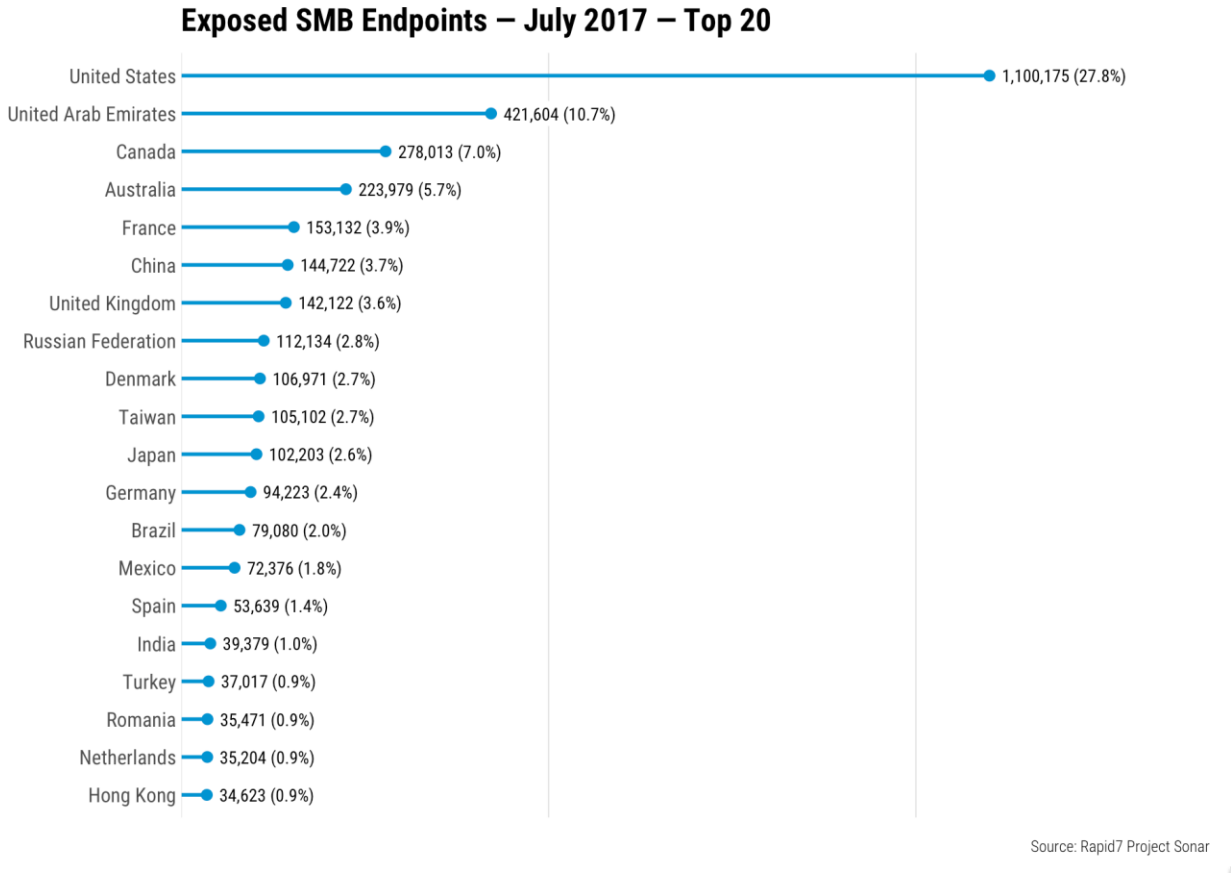
Lesson #2: The opportunities are endless.

Rapid7 Labs' Project Sonar has been performing studies related to the exposure of SMB and RDP to the public Internet for a few years now. These studies are interesting because both of these protocols have checkered histories when it comes to security, and neither should be exposed to the public Internet in an unrestricted manner. There simply is no valid use case for doing otherwise. By studying the exposure of these services over time, we can attempt to gauge patching behavior, security best practices, and more.

The goal of Rapid7's ongoing SMB study is to determine what hosts on the public IPv4 Internet are exposing SMB endpoints and to attempt to gather publicly available information from them. Sonar achieves this first with a zmap scan of ports 139/TCP and 445/TCP and then follows up with an anonymous connection to the SMB endpoint in an attempt to list the available shares, if any. In a recent study, we found over 4 million hosts with one or both of the SMB ports open.

[4]https://community.rapid7.com/community/metasploit/blog/2017/05/17/metasploit-the-power-of-the-community-and-eternalblue
[5]https://www.rapid7.com/info/national-exposure-index/
[6]http://www.zerohedge.com/news/2017-05-16/hackers-sell-second-nsa-developed-cyber-weapon-dark-web
[7]https://support.microsoft.com/en-us/help/4022747/security-update-for-windows-xp-and-windows-server-2003

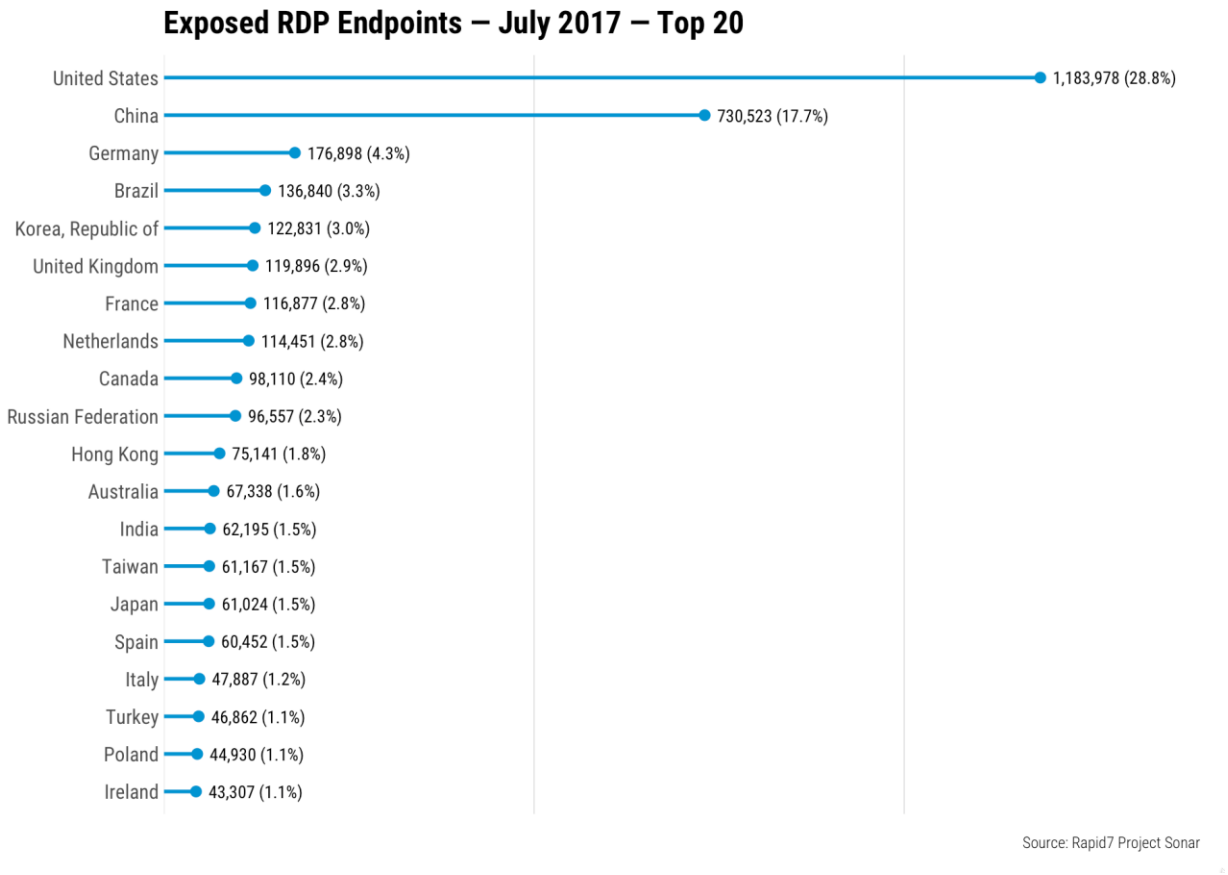
Figure 2: Exposed SMB Endpoints: July 2017, Top 20



The RDP study[8] aims to determine what 3389/TCP endpoints actually appear to be open and speaking RDP. It does so first by finding hosts that have 3389/TCP open, again using zmap. These hosts are then further interrogated by sending only the first in a sequence of packets used in establishing an RDP connection. Any responses that appear to be from an RDP-speaking endpoint are added to the tally of exposed RDP endpoints, and any response that doesn't appear to be valid is saved for future research. In a recent study, we found over 11 million hosts with the RDP port open, and of those we catalogued over 4 million as speaking RDP.

[8] https://scans.io/data/rapid7/sonar.tcp/2017-07-05-1499230861-tcp_rdp.csv.gz

Figure 3: Exposed RDP Endpoints: July 2017, Top 20

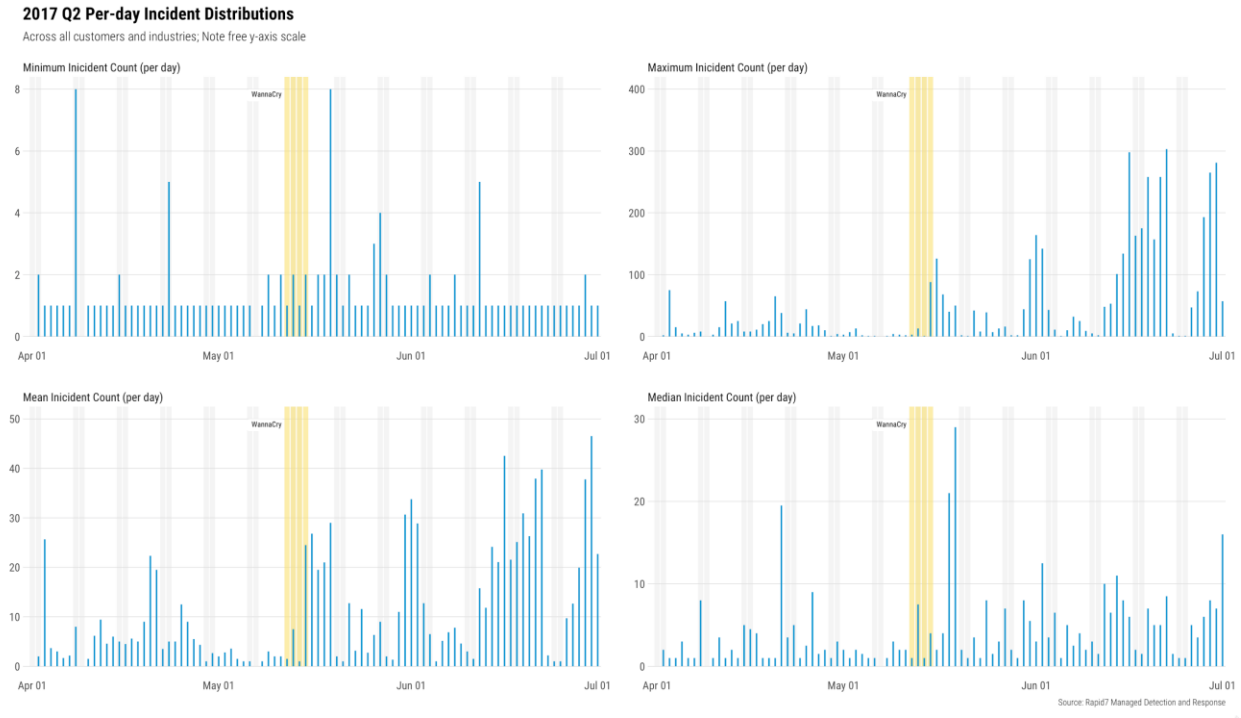


All told, there are several million devices exposing one or more of these services with a questionable security track record. The impending threat of exploitation presents a considerable batch of possible targets for attackers willing to play on that scale.

Lesson #3: The world doesn’t stop when a big attack is in the news.

When WannaCry and NotPetya hit the news, most defenders were almost immediately pulled toward understanding the threat and ensuring that systems were secure. However, during those times, there were still other active threats and other intrusion attempts taking place. During both outbreaks, we continued to see the same tempo of unrelated attacks, including phishing attacks, wire fraud attacks, and bot infections.

Figure 4: 2017 Q2 Per-Day Incident Distributions



Our advice to defenders is to stay vigilant, even when there is a high-profile attack going on. Do not micro-focus on the specific IOCs related to a single event. Instead, look for the opportunities your enterprise is presenting to an attacker (i.e. unpatched vulnerabilities, misconfigurations, etc.), as well as behaviors that indicate not just the individual attack but similar attacks you may see. It is important to understand and communicate the threat your organization faces from breaking news attacks (and act when needed), but so is understanding how an attack fits into the overall threat picture.

A moment for self-reflection: Sizing up **your** threat landscape

As we discussed in the Rapid7 Quarterly Threat Report, 2017 Q1[9], not only does the external threat landscape change as new capabilities are developed (or leaked) and new opportunities are identified, but those changes can also mean different things to different organizations. There are several factors that dictate what threats an organization expects to see.

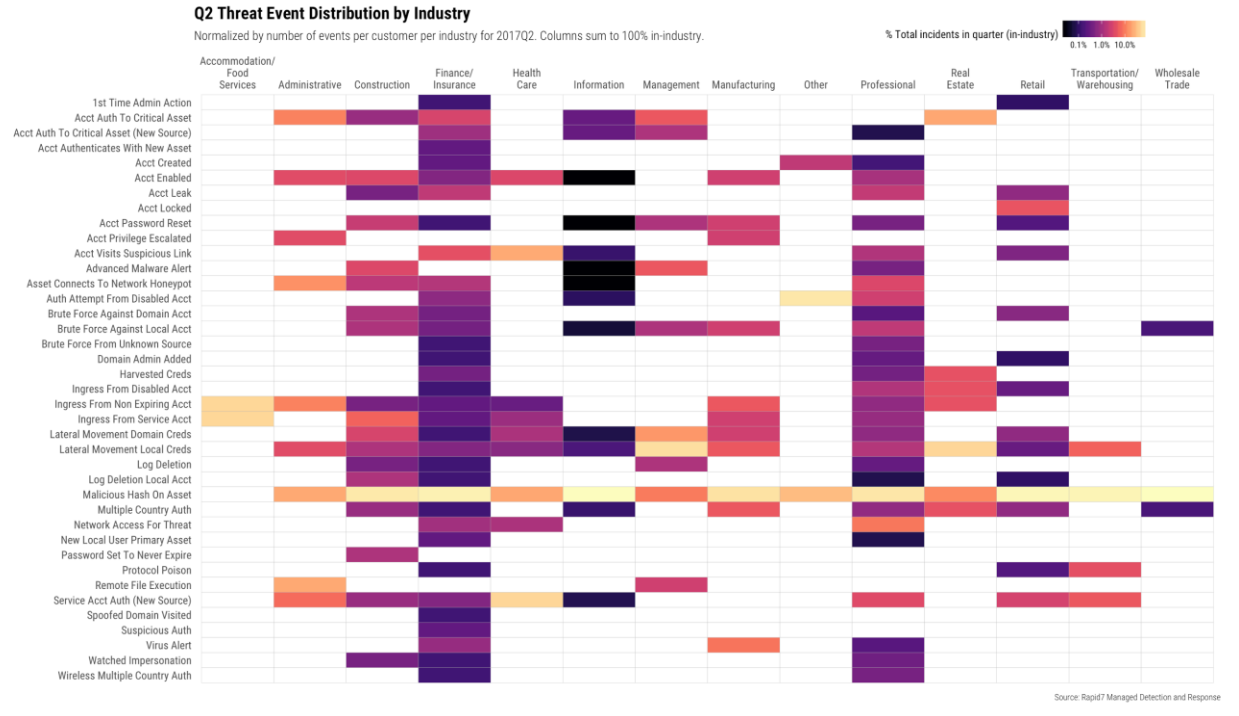
Your Industry

Your specific industry can guide an attacker's intent. Adversaries target specific sectors for the types of information they can get, such as credit card data from the retail sector or intellectual property from the manufacturing sector. In addition, industry-specific devices or equipment also play a role in what opportunities are presented and, therefore, which capabilities can be leveraged against them. Some industries, as well as companies that span several industries,

[9] https://www.rapid7.com/globalassets/_pdfs/research/rapid7-threat-report-2017-q1.pdf

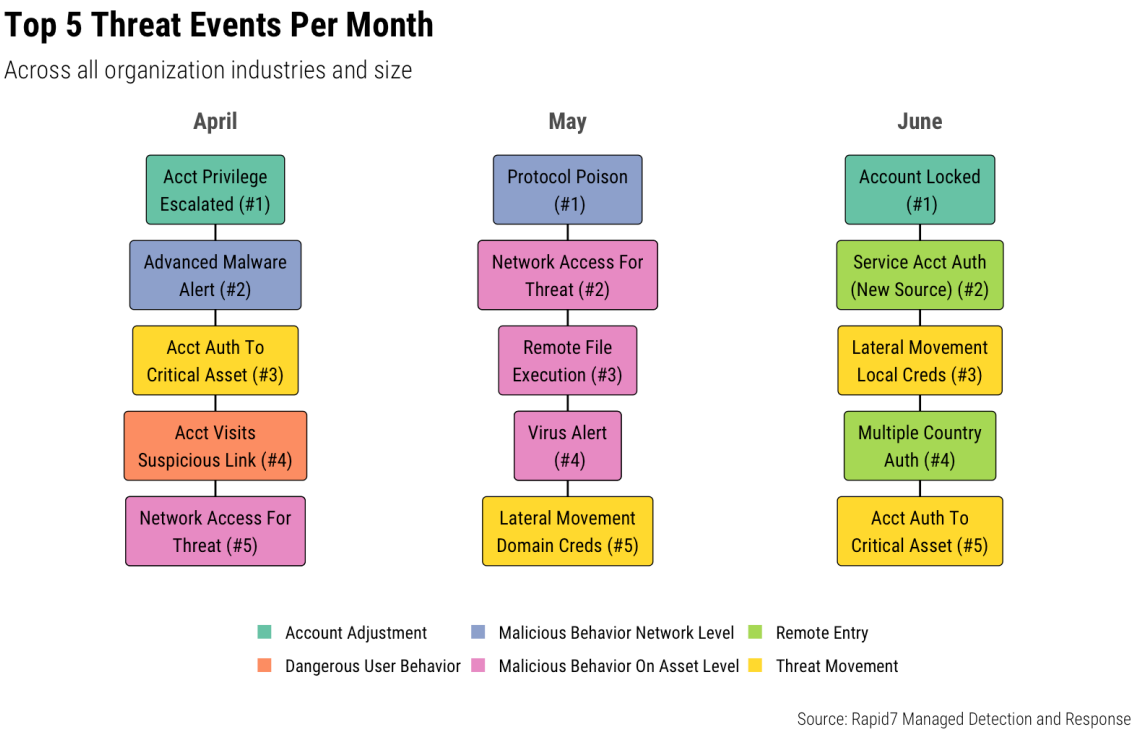
will find themselves with a broad threat landscape, while others have threats concentrated in specific categories.

Figure 5: Q2 Threat Event Distribution by Industry



While there are some threats that are unique to, or more prevalent in, a particular sector or industry, we also saw several categories of threats that were present across a majority of sectors. These are usually related to tactics that are likely to be effective against nearly any organization, including lateral movement and protocol poisoning.

Figure 6: Top 5 Threat Events Per Month

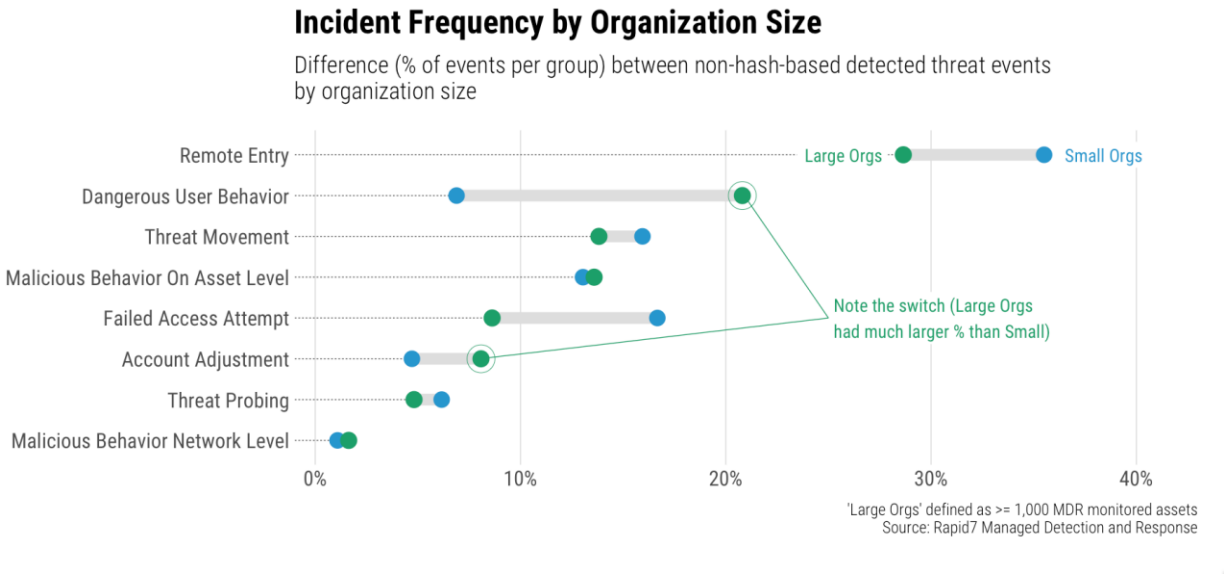


Appendix A has the full breakdown of which InsightIDR events fall into the threat event groups used in Figure 6.

Your Size

It turns out size *does* matter, at least when it comes to network attacks. Large organizations often see different types of attacks than small and medium-sized organizations. While threat categories such as malicious network and endpoint behaviors were very similar in large and small organizations, small organizations had a higher rate of remote entry threats, which include authentication from multiple countries and ingress from a disabled account, while large organizations had a much higher rate of dangerous user behavior, which includes visiting malicious websites, domains, or IP addresses.

Figure 7: Incident Frequency by Organization Size



Our Adversaries

At the end of the day, the adversary is human, which means that, like human defenders, they might not always do things that are predictable or expected. While trends and patterns can help us understand how attackers have operated in the past and, therefore, what we are likely to see in the future, there is always the possibility that an adversary will do something new that defies our previous analysis.

This is one of the primary reasons why we need to stay vigilant to changes in the threat landscape. The combination of a wormable exploit and ransomware was pretty novel, and when attackers combined the two, it had a significant impact on many organizations. Maintaining an awareness of new adversary tactics or targeting will help to ensure that we can keep up with the changing landscape.

Continuing Education

Q2 is behind us (thank goodness!), but we still need to be prepared for the continuation of the trends we saw: attackers leveraging sophisticated capabilities against often overlooked opportunities, such as internet exposed services, that just shouldn't be there.

While defenders must remain vigilant, each headline-grabbing attack should be put into context.

- Don't immediately discount exploits against legacy vulnerabilities—they may have a larger bite than initial bark, especially when dealing with intelligent adversaries.

- Ensure you have a keen understanding of your organization's exposure and attack surface so you can more quickly triage and defend against credible threats.
- Lastly, ensure your incident response program has the flexibility to respond to breaking news while also keeping up with the deluge of your day-to-day attack cadence.

Make sure to keep an eye out for our Q3 threat landscape recap due out in October/November 2017.

Appendix A: Methodology

We gathered up closed and confirmed incidents from across a representative sample of our Managed Detection and Response (MDR) customers using our InsightIDR platform for the second quarter of 2017. Where possible, we've provided full incident counts or percentages; when more discrete information needed to be provided by industry we normalized the values by number of customers per industry. While we wanted to share as much information as possible, the precise number of organizations, industries, and organizations-per-industry is information no reputable vendor would publicly disclose.

As noted in situ, for this report we also incorporated data from both Project Sonar and Heisenberg Cloud. Raw Sonar scan data is available at https://scans.io, and you can contact research@rapid7.com for questions regarding Heisenberg Cloud honeypot data or any other findings or data used in this report.

The following table provides a full breakdown of the InsightIDR threat events and the threat event groups they belong in (as seen in Figure 6). Appendix B has the full, expanded listing of InsightIDR threat events.

IDR Threat Categories:

Dangerous User Behavior

- Account Visits Suspicious Link
- Password Set To Never Expire
- Network Access For Threat

Threat Probing

- Asset Connects To Network Honeypot
- Watched Impersonation

Threat Movement

- Account Authenticated To Critical Asset
- Lateral Movement Domain Credentials

Lateral Movement Local Credentials
Suspicious Authentication

Remote Entry
Wireless Multiple Country Authentications
Multiple Country Authentications
Ingress From Non Expiring Account
Ingress From ServiceAccount
Service Account Authenticated From New Source
Account Authenticated To Critical Asset From New Source
New Local User Primary Asset
Ingress From Disabled Account

Failed Access Attempt
Authentication Attempt From Disabled Account
Brute Force Against Domain Account
Brute Force Against Local Account
Brute Force From Unknown Source

Malicious Behavior On Asset Level
Remote File Execution
VirusAlert
Log Deletion Local Account
Harvested Credentials
Log Deletion
Virus Alert
Network Access For Threat

Suspicious Behavior On Asset Level
Malicious Hash On Asset

Malicious Behavior Network Level
Advanced Malware Alert
Protocol Poison
Administrator Impersonation

Account Adjustment
Account Privilege Escalated
Account Enabled
Account Password Reset
Account Locked
DomainAdmin Added

Appendix B: InsightIDR Threat Events

About Rapid7

With Rapid7, technology professionals gain the clarity, command, and confidence to safely drive innovation and protect against risk. We make it simple to collect operational data across systems, eliminating blind spots and unlocking the information required to securely develop, operate, and manage today's sophisticated applications and services. Our analytics and science transform your data into key insights so you can quickly predict, deter, detect, and remediate attacks and obstacles to productivity. Armed with Rapid7, technology professionals finally gain the insights needed to safely move their business forward. To learn more about Rapid7, visit www.rapid7.com.