RAPID7

RAPID7 RESEARCH

# QUARTERLY THREAT REPORT

By Michelle Martinez, Senior Threat Intelligence Analyst, Rapid7
Kwan Lin, Senior Data Scientist, Rapid7
Bob Rudis, Chief Data Scientist, Rapid7

February 26, 2019

Q4 2018

## TABLE OF CONTENTS

# What Is a Threat?

We throw the term “threat” around a lot, so it’s important to define exactly what it is we mean. When there is an adversary with the intent, capability, and opportunity, a threat exists.

When two or more of these elements are present (e.g., intent and capability, but no opportunity), we call it an impending threat, because there is just one missing piece before it becomes a true threat.

When there is just one element present (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.

# Executive Summary

This issue of the Rapid7 Quarterly Threat Report takes a deep dive into the threat landscape for 2018 Q4 and looks more broadly at 2018 as a whole. We provide an assessment of threat events by organization size and industry, and examine threat incident patterns identified through guidance from security specialists. We also further explore inbound activity to our honeypot network to identify trends and patterns that reveal rising new threats, such as Android Debug Bridge (ADB) activity, the persistence of old threats such as EternalBlue, and the vulnerability posed by non-novel credentials as revealed to publicly exposed systems. The report concludes with five steps you can take to bolster your organization's security posture in 2019 and beyond, based on our findings.

While looking at data on a quarterly basis does reveal interesting patterns, compelling tidbits are also revealed when we aggregate the data into broader sets for analysis. Highlights for 2018 Q4 and 2018 as a whole include the following:

- Continued credential theft and PowerShell use, as well as a look at the most commonly used credential username/password combinations for some popular services;
- A deep dive into our custom Attacker Behavior Analytics rules. We see suspicious authentication as the clear leader here, revealing that attackers are putting those stolen credentials to good use; and,
- A look at some new threats for this year, such as the ADB activity, and some factors that represent a continuation of past patterns, such as attacks directed at port 445/TCP (Microsoft file-sharing over Server Message Block (SMB)).

If there is any consistency in the world of threat events, it is that there will inevitably be change. In 2017, nation-state-grade exploits fell into the hands of every attacker. Based on the data we examined, 2018 was marked by the rise of the deliberate, intelligent adversary who is willing and able to invest in research, development, and diversification. What will happen in 2019? Keep a keen eye peeled for our next quarterly update.

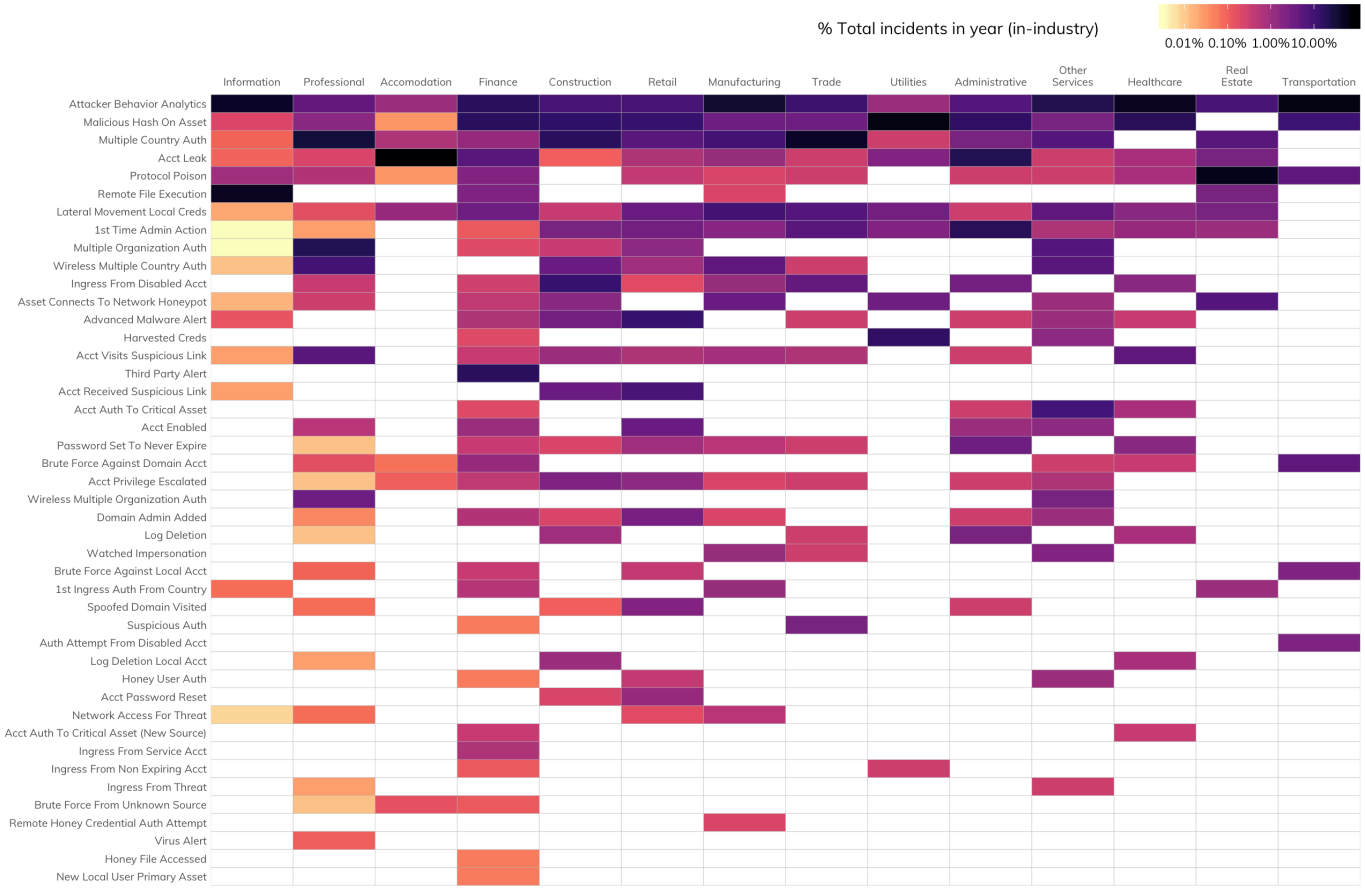
What’s new for this quarter is the rise of the Accommodation industry, which had a high number of events throughout Q4.

# Threat Event Overview

## Industries at a Glance

The industry snapshot for Q4 2018 (Figure 1) reveals a familiar pattern, with high volumes of malicious activity targeting the Information, Professional, and Finance industries. What's new for this quarter is the rise of the Accommodation industry, which had a high number of events throughout Q4. We have seen this particular industry being heavily targeted by attackers, with some high-profile breaches making the news cycle in 2018. This industry is extremely attractive to attackers due to its access to financial and personally identifiable information.

The most prevalent threat events this quarter included triggers from InsightIDR's Attacker Behavior Analytics alert mechanism, malicious hash on assets, and multiple country authorizations, which have slightly overtaken previously seen top threats such as account leakage and protocol poison.




Source: Rapid7 Managed Detection and Response

**Figure 1: Q4 Threat Event Distribution by Industry**

Normalized by total number of events per industry for Q4 2018. Columns sum to 100% in-industry. Threat events and industries arranged in descending order of frequency from left to right, top to bottom.

For more details on what the different threat events entail, check out Appendix B (p.21).

While we typically only provide a quarterly "Threat Event Distribution by Industry" plot, we also included a full-year plot this time around based on an aggregation of all the data collected throughout the year (Figure 2). Over the course of 2018, our Managed Detection and Response (MDR) team encountered many more threat events affecting a broader range of industries. Quite frankly, we were surprised by the increased density of the picture: While quarterly views included a lot of white space, the full-year view was decidedly more colorful, indicating that more industries were exposed to broader ranges of threat events.

**Key Takeaway:** While we certainly do not intend to instill a sense of gloom and doom, it's important to note that any industry is potentially vulnerable to a range of threats, albeit at varying degrees of frequency and severity. Though you may not have encountered a particular threat or may feel safer from particular threats due to your industry, any threat may eventually find its way into your industry.

Granted, certain threats do seem less likely to appear in particular industries based on historical experience. Given constraints, maximizing your overall security posture may require you to judiciously allocate your resources toward addressing security concerns. We suggest using our "Threat Event Distribution" plots as a guide to assess the probability of particular threats appearing in your industry and to take measures to diminish the danger of those threats.

Note that we utilize the North American Industry Classification System (NAICS) as a standard for


Source: Rapid7 Managed Detection and Response

**Figure 2: 2018 Threat Event Distribution by Industry**
Normalized by total number of events per industry for Q4 2018. Columns sum to 100% in-industry. Threat events and industries arranged in descending order of frequency from left to right, top to bottom.

categorizing organizations by industry. If you're unsure of where your organization falls in the industry categorization—especially if you belong to a larger, diversified organization that might be involved in a broad range of functions—perform a search to determine where the NAICS might place your organization.

## Small vs. Large Organizations

Q4 2018 was the first time we've seen Malicious Behavior on Asset taking the lead for threats among larger organizations and Attacker Behavior Analytics coming in as the biggest threat for small organizations. With a rise in malware such as Emotet and Ursnif, our Attacker Behavior Analytics catch a lot of malicious PowerShell.

As in past reports, we grouped threat incidents into broader categories and assessed frequencies separately between small organizations (which we define as organizations with fewer than 1,000 monitored assets) and large organizations (which we define as organizations with 1,000 or more monitored assets).

Over the course of the full year (Figure 4), Remote Entry represented the most common threat event type for both small and large organizations, with small organizations experiencing comparatively more remote entry events. With so many records available from so many breaches in 2018, it makes sense that attackers would transition from reconnaissance and independent credential harvesting to putting their ill-gotten gains to good use.

**Key Takeaway:** While some attackers may pick a target based on size, every single organization has something of value, whether it be actual data such as financial or health records, credential stores, or just plain CPU cycles and network bandwidth to be used for cryptomining or launching other attacks. Though it's important to study the differences outlined in our quarterly updates to see whether your size profile matches our customers' experiences, organizations of all sizes must unfortunately remain vigilant on all fronts, since no company is too small to breach.

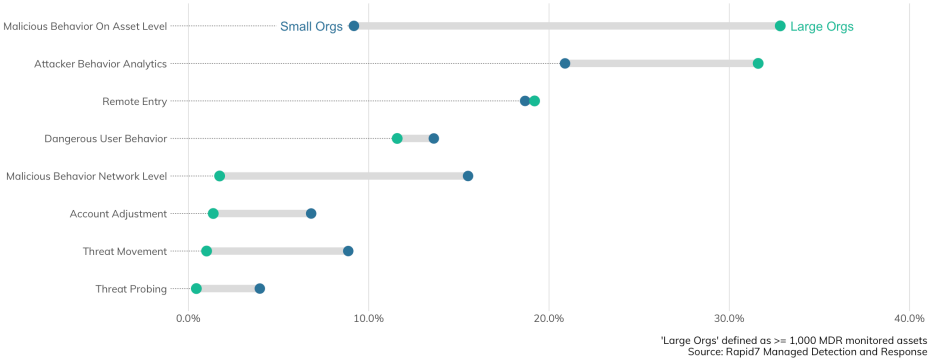



**Figure 3: Q4 Incident Threat Event Frequency**
Percentages represent distributions of detected threat incident groupings within organization size. Ordered by Large Orgs.

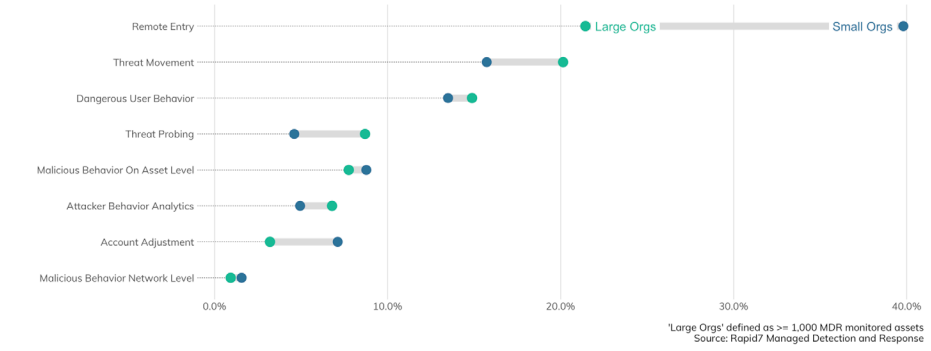



**Figure 4: 2018 Incident Threat Event Frequency**
Percentages represent distributions of detected threat incident groupings within organization size. Ordered by Large Orgs.

## Phishing Fake-Outs Continue

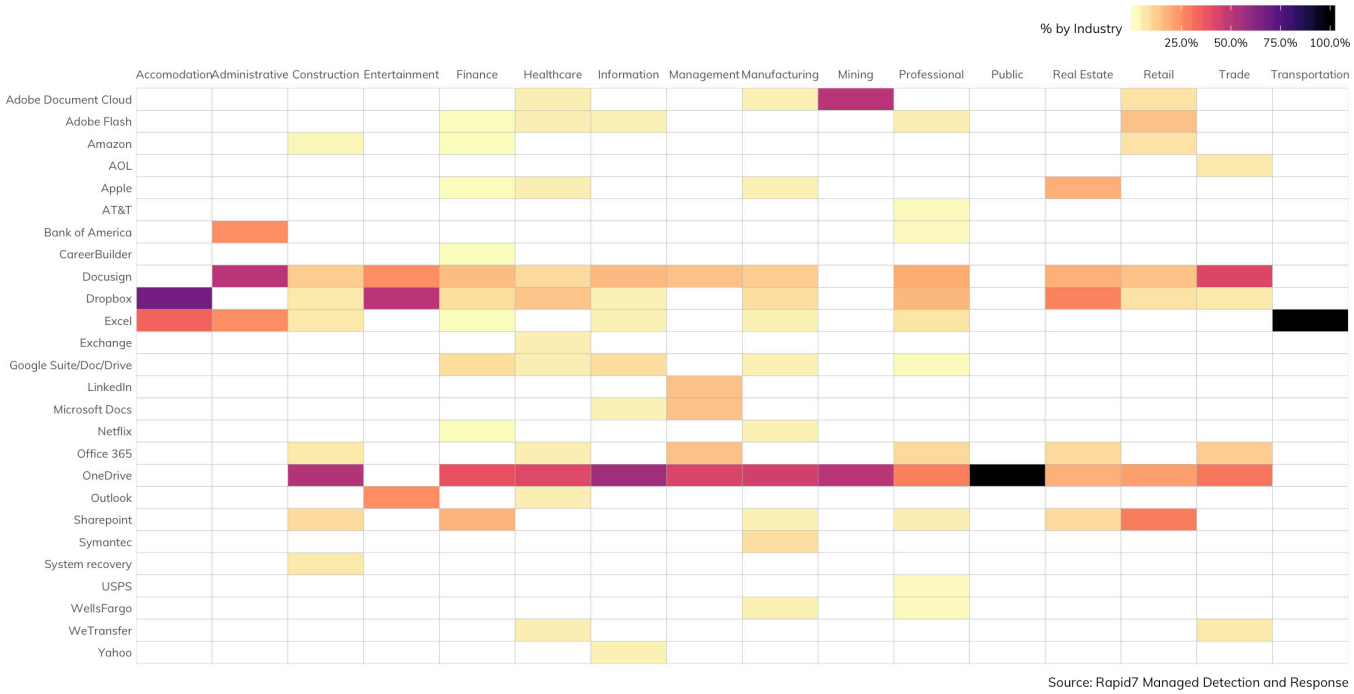
Figure 5 shows that fake service/login lures are still working for attackers, with DocuSign-, Dropbox-, and Microsoft-oriented services being the targets of choice for our corpus.

There are many ways malicious actors can gain remote entry into organizations. One very common method is pilfering legitimate credentials from internal users through spoofed login pages, then utilizing those surreptitiously acquired credentials to enter secure areas.

Different industries may be targeted more or less frequently with different

types of spoofed pages. Services similar to those listed above are spoofed across almost all industry groups, likely because the underlying legitimate services are so widely used. On the other hand, we also see particular spoofed services that really only manifested to notable degrees for particular industries we observed, such as LinkedIn for Management Services. The concentrations of types of spoofed pages can serve as an indicator of what types of login spoofing attempts have been the most effective for different industries in the past.

**Key Takeaway:** Malicious actors try particular techniques at scale because those methods work. They will likely continue to try the same things in the future based on their expectation that their efforts at compromise will bear fruit. You can use the information in the graph to help tailor your employee security training curriculum to better fit your particular industry.




Source: Rapid7 Managed Detection and Response

**Figure 5: Phishing Fake Login Pages by Industry in 2018**
Percentages calculated within industries.

# Improving Detection and Investigation Outcomes with Human-Curated Rules

Over the course of 2018, suspicious authentication was by far the most common group of incidents, followed by indicators based on attackers and PowerShell operations (Figure 6). This falls in line with all of the credential breaches and theft we see happening throughout every industry. We see attackers attempting to log in with stolen credentials, and from there, we can see lateral movement or suspicious processes as they move around the network.

We mention Attacker Behavior Analytics a lot in our reports, but for this year-end report, we wanted to take a deeper dive into breaking these rules out to get more granularity into what exactly we're seeing. Our MDR team maintains a set of custom rules distinct from the conventional base of rules built into the InsightIDR platform. Those custom rules manifest as a result of idiosyncrasies in the customers served by MDR and the experiences of our MDR analysts.

As with the threat event analysis and size-based analysis, we similarly separate the custom rules groups by industry (Figure 7).

Many of the threat incident groupings were fairly egalitarian in the sense that they affected diverse industries—albeit with varying degrees of frequency. However, there were some incident groupings that were proportionately more common for particular industries. When we look at the data vertically by industry, we see that some industries encountered almost all the threat categorizations (e.g., Financial Services, Information Services), while other industries encountered a fairly limited set (e.g., Mining, Public Services).

**Key Takeaway:** Regardless of the level of "artificial" intelligence that's baked into any given security event information management (SIEM) system you may use, you will absolutely achieve better outcomes in detecting, deterring, and investigating incidents if you incorporate key learnings by your incredibly smart human responders into your processes.

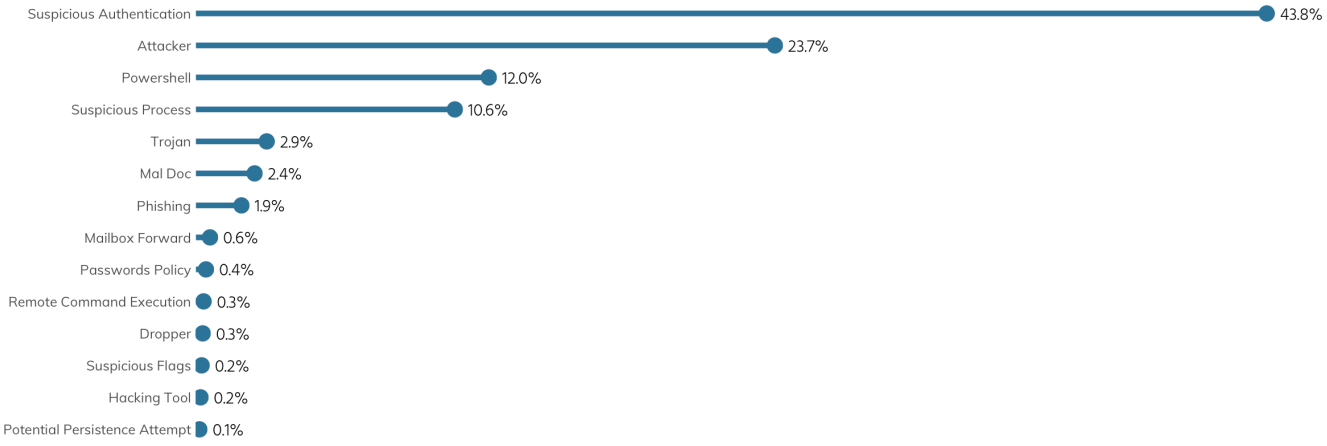
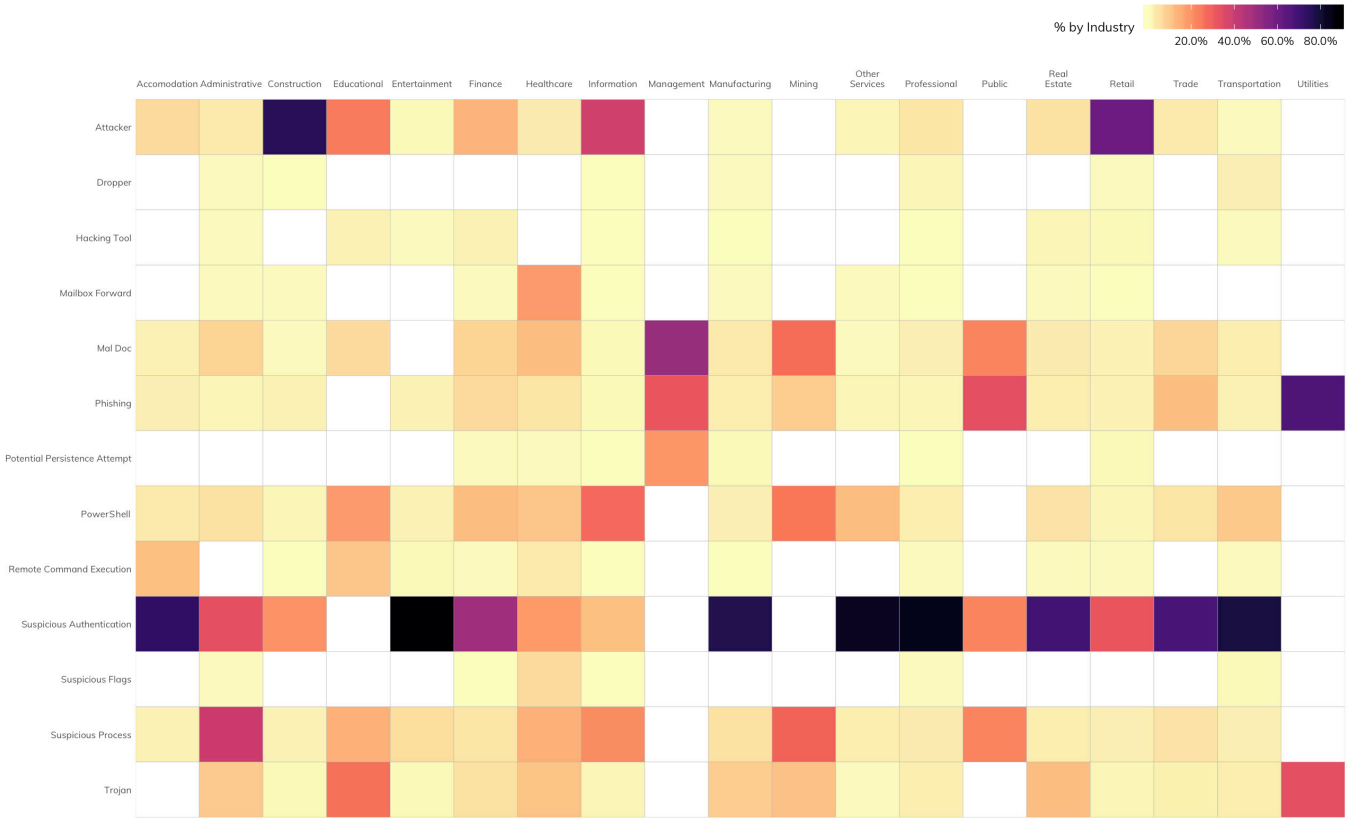



**Figure 6: Custom Indicator Groups in 2018**
Low frequency custom indicator groups removed.




Source: Rapid7 Managed Detection and Response

**Figure 7: 2018 Custom Rules–Incidents by Industry**

Percentages calculated within industries. Infrequent incident types excluded.

# Take a Day or Two Off to Avoid Phishing Attacks

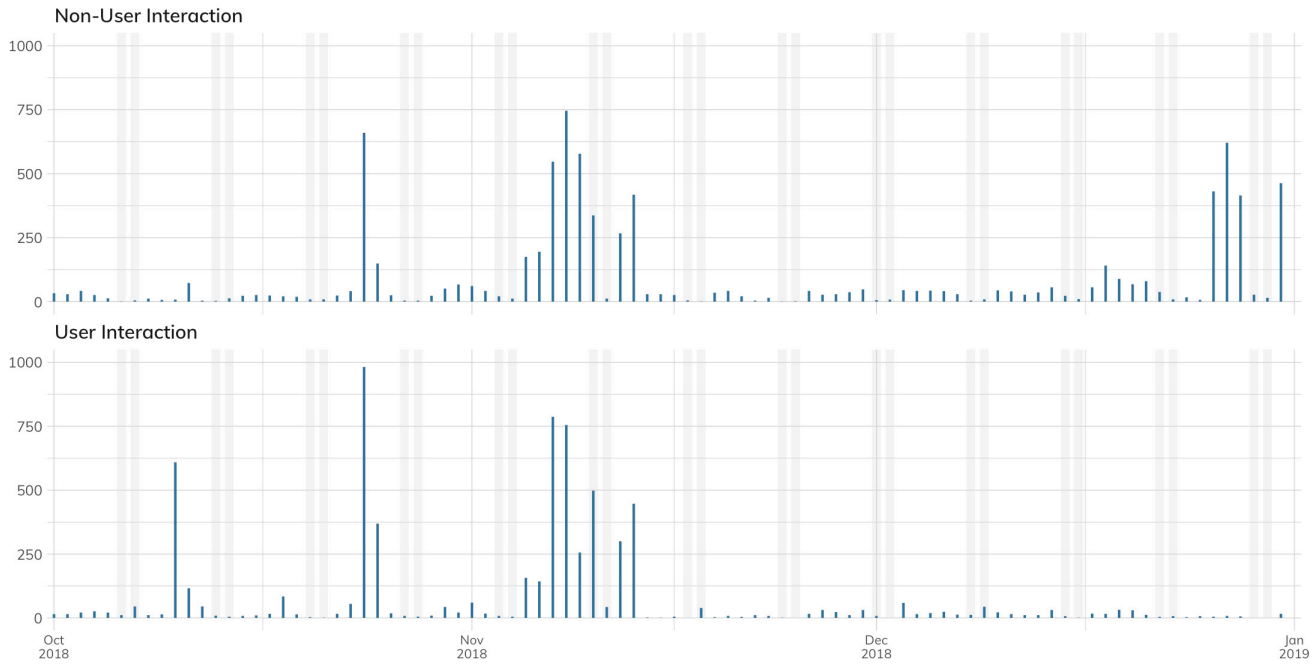
In the 2018 Q3 Threat Report[1], we introduced a view to show threat incidents that required user interaction (such as dangerous user behavior) alongside threat events that did not require user interaction (such as system misconfigurations). Our Q3 report covered the summer, and we noticed a comparative drop in user interaction incidents.

Our hypothesis at the time was that this drop in user interaction events was due to summer holidays and environmental events that affected U.S. organizations (which represent the bulk of our MDR data). Our theory was that once the summer season had passed and organizations returned to business as usual, the user interaction and non-user-interaction incidents would equalize.

The data we collected this past quarter seems to support our initial hypothesis: Aside from a few non-systematic spikes for both non-user and user interaction events, broad categories of incidents followed fairly common patterns around incident frequency (Figure 8). Therefore, it appears to be true that the summer was slower due to employee absences.

In most U.S. organizations, the tail end of the year is often just as inactive as the summer period due to winter holidays. Many offices are closed, and most employees are on vacation. We could hypothesize that like the summer period, the winter holiday period is likely to experience lower frequencies of incidents that involve user interaction, which does appear accurate based on our analysis in Figure 8.

**Key Takeaway:** Segmenting your own incidents into "interactive" versus "non-interactive" will help you understand your own threat profile and tailor your defenses and response plans accordingly. If you are a fairly large organization with "traditional" business processes and do not see the same interactive pattern, we'd definitely like to hear from you at research@rapid7.com.




Source: Rapid7 Managed Detection and Response

**Figure 8: Q4 Incident Distributions**
Across all organizations and industries. Gray bars represent weekends.

1 "Rapid7 Q3 Threat Report," https://www.rapid7.com/info/threat-report/2018-q3-threat-report/

Rapid7 Labs started to see low-and-slow probes for open ADB ports in February...

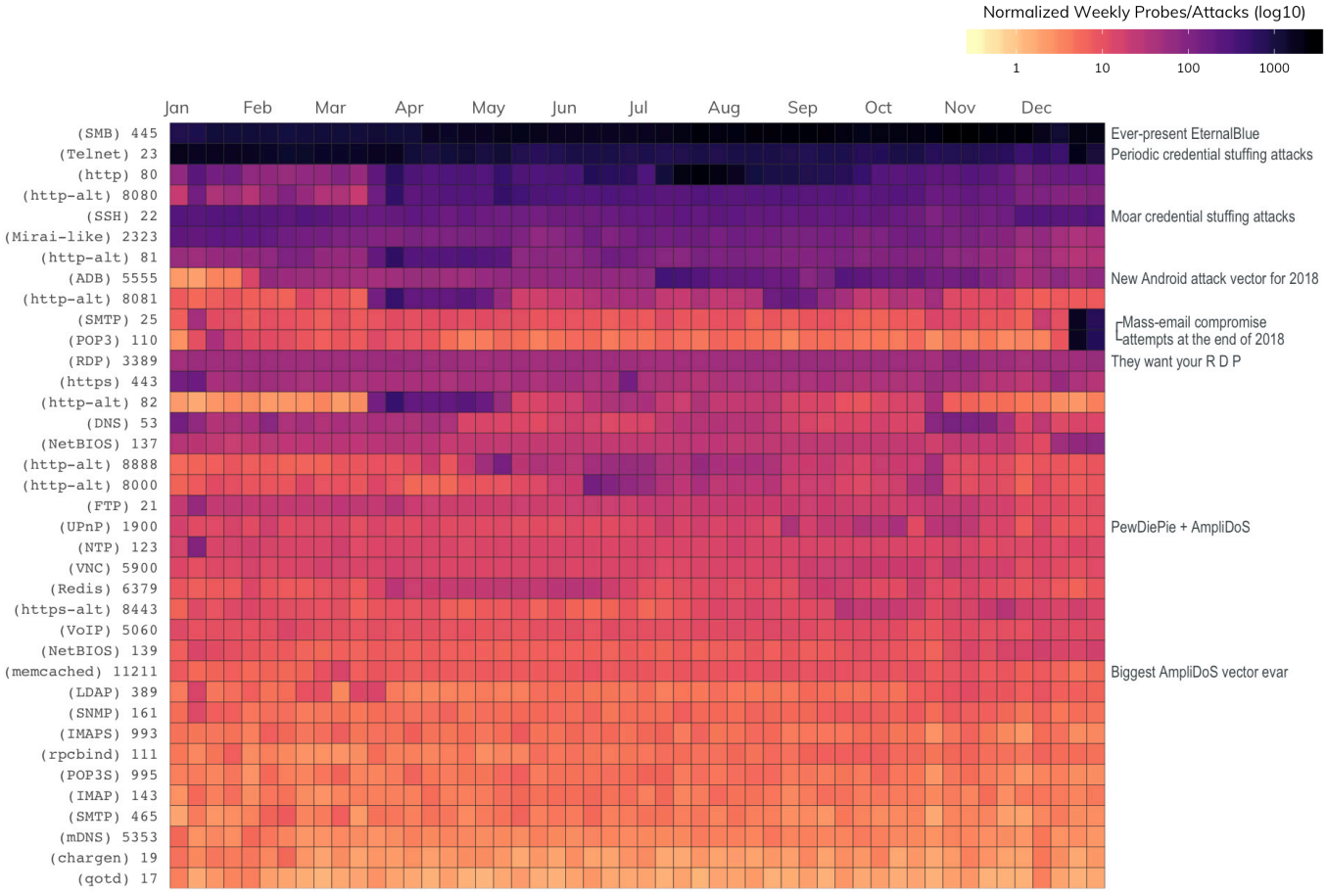
# 2018: A Look in the Rearview Mirror

The past year was a busy one for both attackers and defenders. As we all drive fast and furious into 2019, let's take a minute to check the rearview mirror to see whether there are any lessons we can carry forward based on deep dives on particular trends.

## I Can't Drive 5555

Port 5555/TCP, home to the ADB, became a new vector of choice for aspiring cryptominers[2] looking to turn a profit off of illicit IPTV boxes[3] and any other Android devices with an open ADB port. As seen in Figure 10, Rapid7 Labs started to see low-and-slow probes for open ADB ports in February, followed by bursts of activity throughout the remainder of the year and a volume spike in July that surprised most of the cybersecurity community (including us).

Keen observers will notice the downward trend starting in late October and may be quick to judge that this area of focus may have just been a fad. Sadly, the downturn was due to reseller and legislative action[4] in numerous countries that outlawed the use of pirate IPTV boxes and forced




Source: Rapid7 Project Heisenberg & GreyNoise Intelligence

**Figure 9: 2018 Attack Map**

Each square is filled according to the number of normalized (per-sensor) unique probes/attacks caught by Rapid7 Labs' Heisenberg Sensor Network. Port/protocol ordered by highest activity to lowest.

2 360 NetLab ADB Investigation — http://blog.netlab.360.com/adb-miner-more-information-en/

3 Root Bridge—how thousands of internet connected Android devices now have no security, and are being exploited by criminals. — https://doublepulsar.com/root-bridge-how-thousands-of-internet-connected-android-devices-now-have-no-security-and-are-b46a68cb0f20

4 Kodi in steep decline after introduction of anti-piracy steps — https://www.comparitech.com/kodi/kodi-piracy-decline/

service providers to clamp down on offenders. That's right, you can thank intellectual property lawyers for helping to stop cyber-crime.

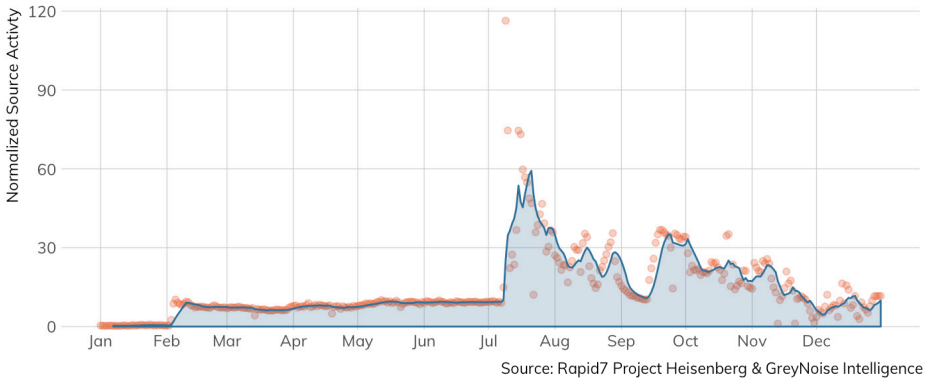



**Figure 10: 2018 Android Debug Bridge Activity**
Daily normalized source counts (orange) with seven day moving average (blue).

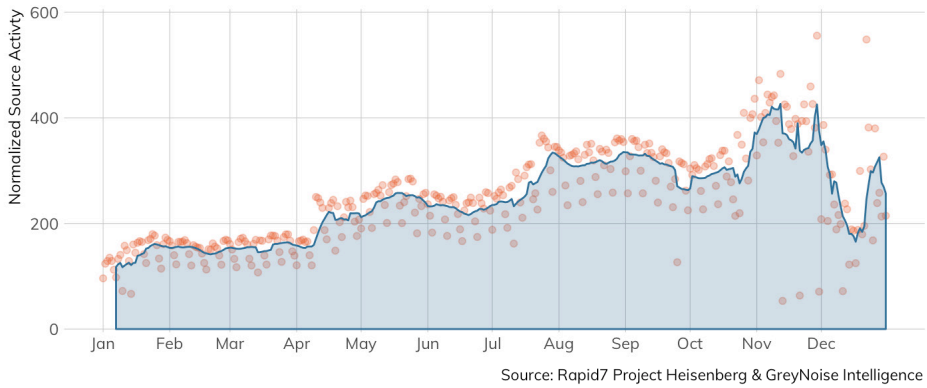



**Figure 11: 2018 EternalBlue (Microsoft SMB) Activity**
Daily normalized source counts (orange) with seven day moving average (blue).

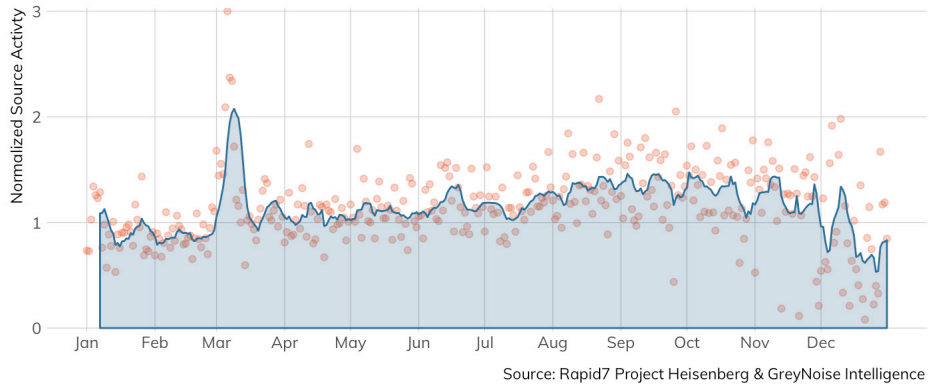



**Figure 12: 2018 memchached Activity**
Daily normalized source counts (orange) with seven day moving average (blue).

**Key Takeaway:** Be mindful of new threat vectors. This was the first of many examples of attackers showing their skill, creativity, and flexibility when it comes to discovering and exploiting new areas of attack. After the surprise spike in ADB activity in July, we were able to retrospectively spot the slow and steady traffic that started back in February that ultimately culminated in this new attack vector.

## Attackers Still Getting Good Mileage Out of EternalBlue

If the main theme of the ADB/port 5555 story was "Attackers are innovating," the theme of the TCP/port 445 (Microsoft File-Sharing/SMB) story is "We'll stick with what works." The first thing to focus on in the 2018 EternalBlue chart is how steady the seven-day moving average growth is.

Our reports have noted that many attackers operate like a nine-to-five, Monday–Friday business, and the SMB probe and attack profile fits squarely into this model. It's also important to note that we say "growth" here because that's all malicious SMB traffic profiles have done since the Shadow Brokers released their ill-gotten exploits into the wild. The code has been repurposed from freshman-level ransomware (WannaCry) to grad-school-level enterprise-crippling attack kits (NotPetya), to MBA-level cryptomining (and everything in between). It's truly the gift that keeps on giving.

The final thing you should note from the chart is that our Project Heisenberg honeypot network had some occasional and unexpected regional downtime starting in November that temporarily reduced our visibility into these attacks. So, don't interpret the dip as a reduction

in attack levels, since they are now back up to following the growth path.

**Key Takeaway:** Keep focusing on the fundamentals. Just like you're supposed to do a quick systems check before heading out of your driveway, you need to have an up-to-date inventory of your assets, make sure critical patches are deployed quickly, and check that secure configurations are in place. Finally, do everything you can to prevent woefully insecure devices such as Microsoft SMB from being deployed directly on the internet.

## Tireless memcached Traffic

No cybersecurity report covering 2018–2019 would be complete without at least one mention of the 2018 memcached GitHub distributed denial-of-service (DDoS) attack,[5] so here we are. Attacker groups kept combing the internet in 2018 for nodes they could use in this new, powerful memcached amplification attack vector, and this activity steadily grew throughout the year, as seen in Figure 12.

The flux you see at the end of the year is, again, due to regional glitches noted in the "Attackers Still Getting Good Mileage Out of EternalBlue" section. In fact, attackers refreshed their inventory lists across all amplification DDoS ports/services because DDoS is both a useful distraction tool and remains profitable in the stresser/booter black market industry.[6] Rest assured that denial-of-service (DoS) attacks will continue to plague individuals and organizations throughout 2019 despite a successful takedown[7] of DDoS-as-a-Service[8] sites in December by the U.S. Federal Bureau of Investigation (FBI).

**Key Takeaway:** Invest in DDoS mitigation and keep one hand on the data-wheel at all times. If your organization relies on employee internet access to conduct business-critical processes or your internet-facing sites are a critical component of your profit margins, you absolutely need to have a plan in place and ready to deploy if you become the victim of a DoS attack. You also need to ensure you have DoS attack response plans in your SecOps playbook. These plans must cover cases in which DoS is the direct attack (i.e., you're being hit with a DDoS attack by a competitor for spite or ransom), especially when they're designed to distract your scant security resources while attackers make off with your data.

## License and Credentials, Please

Many of the services present on the 2018 Attack Map are especially vulnerable to credential stuffing[9] attacks—the automated injection of breached username/password pairs in order to fraudulently gain access to user accounts. There are now upward of 1.5 billion credentials floating in the wild ready for use by malicious miscreants at an exposed service near your data. The treemaps in Figure 13 show the top usernames (in black) and password combinations for six of the most common services. That means admin/admin was, sadly, the top pair for HTTP and root/1234 was the top pair for Telnet.

Attackers try these because, well, they work. A significant percentage of routers, switches, and servers are left addressable on the internet, and these common default credential settings are just waiting to be abused. The table below shows the total number of unique username/password pairs.

| SERVICE | UNIQUE CREDENTIALS |
|---|---|
| http | 544 |
| mssql | 14104 |
| mysql | 5951 |
| rdp | 8275 |
| ssh | 88464 |
| telnet | 5871 |

## Map Your Own Adventure

If the 2018 Attack Map and the curated selection of stories from it has piqued your interest, you can play along at home by heading over to the Rapid7 Labs GitHub repo[10] and examining the charts for all the ports featured in the heatmap. Can you spot the PewDiePie-inspired UPnP[11] bursts? Did your websites see the same increased levels of activity as noted in the HTTP Port 80[12] profile?

5 "The Flip Side of memcached", https://blog.rapid7.com/2018/02/27/the-flip-side-of-memcrashed/
6 "What is a DDOS Booter/IP Stresser," https://www.cloudflare.com/learning/ddos/ddos-attack-tools/ddos-booter-ip-stresser/
7 "FBI swoops on 'national threat' 'hacks for hire' sites," https://www.bbc.com/news/technology-46647390
8 DDSAAS is the worst Scrabble tile-hand, ever.
9 OWASP Credential Stuffing Explained , https://www.owasp.org/index.php/Credential_stuffing
10 2018 Q4 Threat Report Extras https://github.com/rapid7/data/tree/master/threat-report/extras/2018-q4-extras
11 UPnP Port 1900 https://github.com/rapid7/data/blob/master/threat-report/extras/2018-q4-extras/upnp-1900.png
12 HTTP Port 80 https://github.com/rapid7/data/blob/master/threat-report/extras/2018-q4-extras/http-80.png


Source: Rapid7 Heisenberg Cloud

**Figure 13: 2018 Credentials Attempted**

Percentages calculated within protocols across aggregated top 10 usernames and 10 passwords of the usernames subset. Grids scaled by log10.

# Conclusion

Based on the analysis we've performed using MDR, Heisenberg, and other public data sources, here are five steps you can take to bolster your security posture in 2019 and beyond:

1. Use our Threat Event Distribution by Industry (p.8) as a guide to figure out which threat events are most probable for your industry, then tailor your security measures accordingly.

2. Be wary of new threat vectors. If you have astutely addressed all known threats, great! But that still doesn't mean that you've secured yourself against every potential vector of attack.

3. Be wary of old threat vectors. Just because certain attack methods have been tried in the past doesn't mean they aren't still a threat. Attackers often find old methods just as reliable today as when they first appeared.

4. Ditch simple, user-generated passwords and make the adoption of risk-based, two-factor authentication a priority for your organization in 2019.

5. ~~Fire all your employees.~~ Your humans are both your organization's greatest assets and, unfortunately, the prime attack vector for attackers. Heed the knowledge gained and reinforced about attackers relying on humans to focus on enabling your workforce to be co-defenders of your enterprise. They power your business processes and should be your best partners when it comes to defense. Give them the data and the knowledge they need to make better decisions and recognize sketchy links or sites. Support this work by having transparency at every level of your organization, since attackers rely on urgency and overbearing corporate cultures to make their phishing attacks work. Without appropriate guidance, your greatest asset might just be your greatest liability.

The internet is a wonderful but dangerous place. We hope that by arming you with data-driven knowledge, you can better secure your organization against the persistently roaming threats in the digital wilderness.

**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 solution for the fourth quarter of 2018. 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.

Additionally, we also used coded incident data provided by our MDR incident responders. Each coded incident contains one or more alerts from the raw event data, along with an incident narrative. We refer to these as "significant investigations," and they help capture the stories that the discrete alerts tell.

As noted in situ, for this report we also incorporated data from both Project Sonar and Project Heisenberg. Raw Sonar scan data and limited Heisenberg data is available at no cost via httpd://opendata.rapid7.com/, and you can contact research@rapid7.com for questions regarding those data sources or any other findings/data used in this report. Known benign traffic was filtered out of all honeypot data using feeds provided by GreyNoise Intelligence (https://greynoise.io/#rapid7).

The following table provides a full breakdown of the InsightIDR threat events and the threat event groups they belong in (as seen in Figure 1). 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
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

| EVENT | DESCRIPTION |
|---|---|
| Account Authenticated To Critical Asset | A new user authenticates to a restricted asset. |
| Account Authenticated To Critical Asset From New Source | A permitted user authenticates to a restricted asset from a new source asset. |
| Account Authenticates With New Asset | A permitted user is authenticating to an application from a new source asset. |
| Account Created | An account was created on a flagged asset. |
| Account Enabled | A previously disabled user account is re-enabled by an administrator. |
| Account Leak | A user's credentials may have been leaked to the public domain. |
| Account Password Reset | A user resets the password for an account. |
| Account Privilege Escalated | An administrator assigns higher level of privileges to the account. |
| Account Received Suspicious Link | A user receives an email containing a link flagged by the community or threat feeds. |
| Account Visits Suspicious Link | A user accesses a link URL identified as a threat from the Threats section or from other intel sources. |
| Advanced Malware Alert | An advanced malware system generates an alert. |
| Asset Connects To Network Honeypot | There was an attempt to connect to a network honeypot. |
| Attacker Behavior Analytics | A pre-built detection modeled around intrustion analysis and threat intelligence findings was triggered. |
| Authentication Attempt From Disabled Account | A disabled user attempts to access an asset. |
| Brute Force Against Domain Account | A domain account has failed to authenticate to the same asset excessively. |
| Brute Force Against Local Account | A local account has failed to authenticate to the same asset excessively. |
| Brute Force From Unknown Source | An unknown source has failed to authenticate to the same asset excessively. |
| Domain Admin Added | A user has been added to a privileged LDAP group. |
| First Ingress Authentication From Country | A user logs onto the network for the first time from a different country. |
| First Time Admin Action | An administrator action was used for the first time in this domain. |
| Harvested Credentials | Multiple accounts are attempting to authenticate to a single, unusual location. |
| Ingress From Disabled Account | A disabled user logs onto the network or a monitored cloud service. |
| Ingress From Non Expiring Account | An account with a password that never expires accesses the network from an external location. |
| Ingress From Service Account | A service account accesses the network from an external location. |
| Lateral Movement Domain Credentials | A domain account attempts to access several new assets in a short period of time. |
| Lateral Movement Local Credentials | A local account attempts to access several assets in a short period of time. |
| Log Deletion | A user deletes event logs on an asset. |
| Log Deletion Local Account | A local account deletes event logs on an asset. |
| Malicious Hash On Asset | A flagged process hash starts running on an asset for the first time. |
| Multiple Country Authentications | A user accesses the network from several different countries within a short period of time. |
| Multiple Organization Authentications | A user accesses the network from multiple external organizations too quickly. |
| Network Access For Threat | A user accesses a domain or IP address tagged in the Threats section. |
| New Local User Primary Asset | A new local user account was added to the primary asset of a domain user. |
| New Mobile Device | A user accesses the network from a new mobile device. |
| Password Set To Never Expire | A password of an account has been set to never expire. |
| Protocol Poison | Poisoning of a network protocol, such as via Responder, is detected. |

| EVENT | DESCRIPTION |
| --- | --- |
| Remote File Execution | Remote file execution has been detected. |
| Service Account Authenticated From New Source | A service account authenticates from a new source asset. |
| Spoofed Domain Visited | A user makes a DNS query to a newly registered internet domain. |
| Suspicious Authentication | A suspicious authentication was detected. |
| Virus Alert | A virus alert was triggered from an asset. |
| Watched Impersonation | A user authenticates to a watched user's account. |
| Wireless Multiple Country Authentications | A user logs onto the network using a mobile device from too many countries in a short period of time. |

# About Rapid7

Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Customers around the globe rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations. For more information, or to get involved in our threat research, visit www.rapid7.com.

## QUESTIONS?

Email us at research@rapid7.com

RAPID7