RAPID7

RAPID7 RESEARCH

QUARTERLY THREAT REPORT

By Rebekah Brown, Threat Intelligence Lead, Rapid7, Inc.
Kwan Lin, Senior Data Scientist, Rapid7, Inc.
Bob Rudis, Chief Data Scientist, Rapid7, Inc.

Q2 2018

August 21, 2018

CONTENTS

WHAT IS A THREAT?

We throw the term “threat” around a lot, and 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.

INTRODUCTION

Summer is in full swing, and while many people spend these months taking time off to travel, relax, or head to Hacker Summer Camp[1] in the sweltering Las Vegas sun, networks are still at risk and need to be defended. In the second quarter of 2018, we continued to see high levels of activities aimed at identifying and compromising systems of interest, whether the attackers' plan was to steal financial information or, as we see more and more, steal other sensitive information such as credentials that can be used for a variety of information-based operations.

The good news is that even though there has been a shift in motivations and how stolen information is used, many of the tactics being used to achieve these goals are not changing as drastically. Other highlights of 2018 Q2 include:

- We saw a continued emphasis on credential theft and account leaks across all industries, along with an increase in remote access attempts.
- In addition to Microsoft's Server Message Block (SMB) protocol, adversaries demonstrated interest in Microsoft's Remote Desktop Protocol (RDP), with many of the access attempts utilizing brute force methods for gaining access.
- Botnet wranglers definitely did not take any vacation time in Q2. Our Heisenberg[2] honeypot nodes caught numerous attempts to inventory and usurp various devices and services this quarter, including campaigns against a cadre of routers, Android debugger-enabled systems, Drupal, and WebLogic.

Read on for more of what we saw in the second quarter of 2018, and what it means for the rest of the year.

---

[1] https://www.defcon.org/

[2] https://www.rapid7.com/research/project-heisenberg/

Q2 of 2018 saw a return to the patterns of a year ago: The finance, professional, and information sectors had the highest volume and most variety of malicious activity.

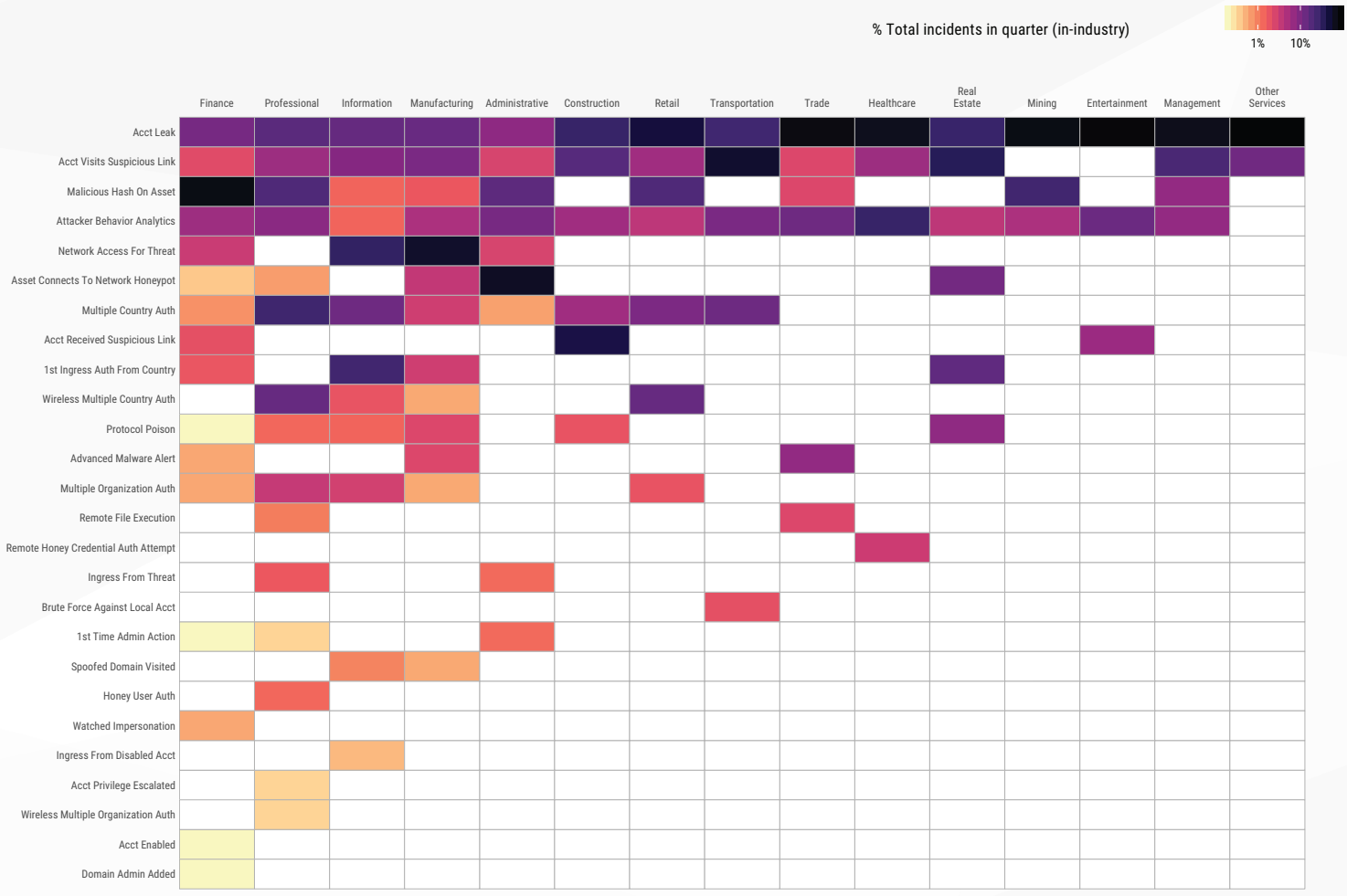
Threat Event Overview

Industry Snapshot

After a few quarters of interesting trends in industry targeting, Q2 of 2018 saw a return to the patterns of a year ago: The finance, professional, and information sectors had the highest volume and most variety of malicious activity. The manufacturing sector also had a high number of events, consistent with the steady rise in targeting that we have seen toward that industry over the past few quarters.

Figure 1: Q2 Threat Event Distribution by Industry

Normalized by number of events per organization per industry for Q2 2018. Columns sum to 100% in-industry.



Source: Rapid7 Managed Detection and Response

Retail organizations also saw an increase in activity in Q2. Along with regular intrusion attempts across the majority of industries, we saw two detections based on InsightIDR[3] user behavior analytics (UBA) that indicate how attackers are attempting to gain access using legitimate credentials: authorizations from multiple countries and external organizations.

[3] https://www.rapid7.com/products/insightidr/

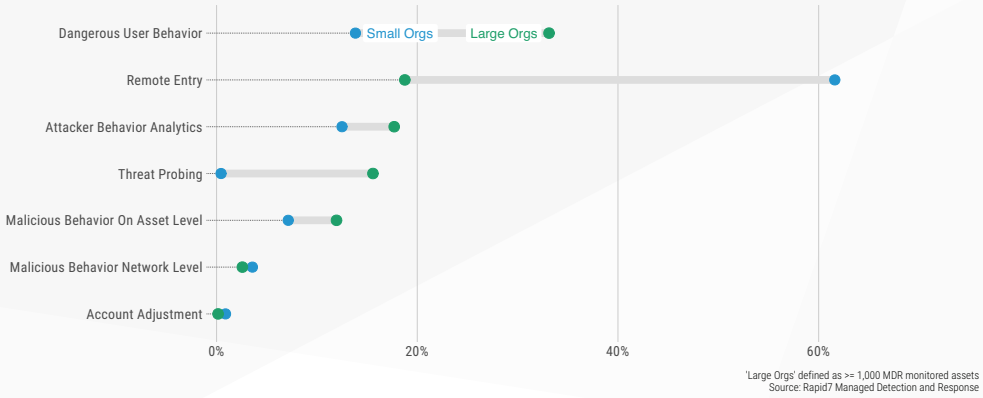
Authentications from multiple countries or organizations within a short period of time can indicate that an adversary with legitimate credentials (either from an employee or from a trusted partner) is trying to use those credentials to gain access to the network. These credentials often come from password dumps; they are leveraged by adversaries specifically targeting an organization with connections from and access to a variety of companies, similar to what was seen in the Cloud Hopper campaign[4] from 2017. Although we typically see a handful of these types of authorizations at any given time, there was a significant increase in these attempts from mid-May to the beginning of June.

Threat Frequency by Organization Size

Remote entry took the lead this quarter, accounting for more than half of the activity targeting small organizations (defined as organizations with fewer than 1,000 employees). While remote entry also made up a significant amount of the activity targeting large organizations, the top incident type we saw facing large organizations in Q2 was dangerous user behavior. We also observed that dangerous user behavior is directly tied to the potential for attackers to attempt more remote entry attacks against these organizations moving forward, as users visit URLs designed to steal credentials. The majority of credential theft URLs were directed against large organizations. The top sectors hit by these credential theft campaigns were information, finance, and manufacturing.

Figure 2: Q2 Incident Threat Event Frequency

Percentages represent distributions of detected threat incident groupings within organization size.

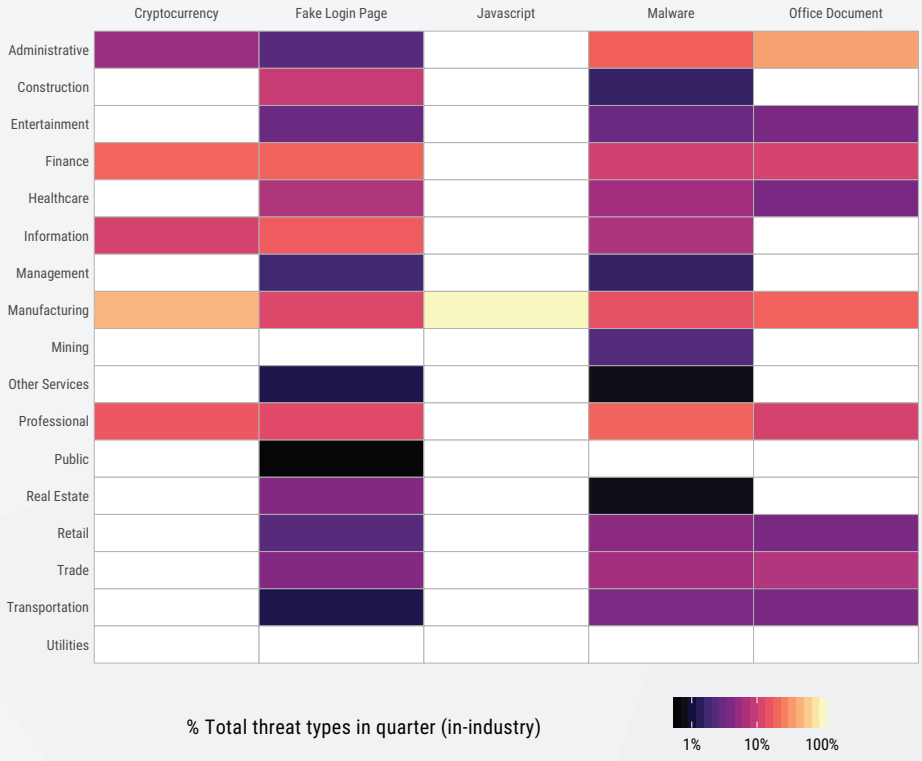


'Large Orgs' defined as >= 1,000 MDR monitored assets
Source: Rapid7 Managed Detection and Response

[4]https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper.html

Figure 3: Q2 Threat Type Distribution by Industry

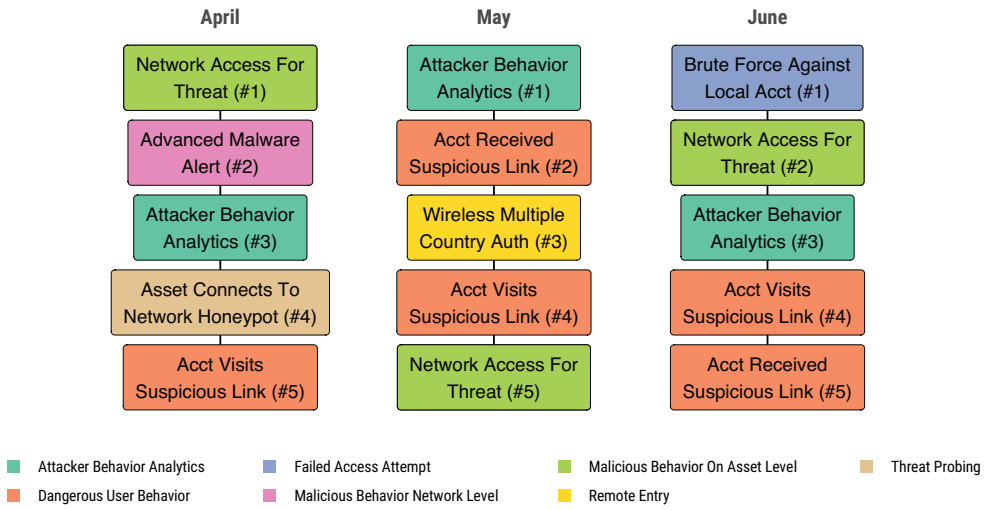
Normalized by number of threat types per industry for Q2 2018. Columns sum to 100% in-industry.



Source: Rapid7 Managed Detection and Response

Figure 4: Top 5 Threat Events Per Month

Across all organizations



Source: Rapid7 Managed Detection and Response

In Q2, we launched a new detection method in InsightIDR, Attacker Behavior Analytics, which was derived from the excellent work done by our Managed Detection and Response Security Operations Center (SOC). Attacker Behavior Analytics are pre-built detections modeled around a wide array of intrusion analysis and threat intelligence findings. Aimed at identifying activity that has historically been associated with specific attacker techniques[5], these analytics also cover a range of activity associated with cryptomining, credential theft, and malicious powershell usage. Attacker Behavior Analytics were responsible for many of the validated alerts that our Managed Detection and Response team tracked in Q2, taking the top spot in May. Overall, however, activities associated with user interaction, such as users visiting suspicious links, were also a consistent factor in the top threats for Q2.

[5] https://www.rapid7.com/solutions/attacker-behavior-analytics/

Brute force attacks are linked to recent attacks such as SamSam ransomware, which has targeted the healthcare sector as well as state and local governments in past quarters.

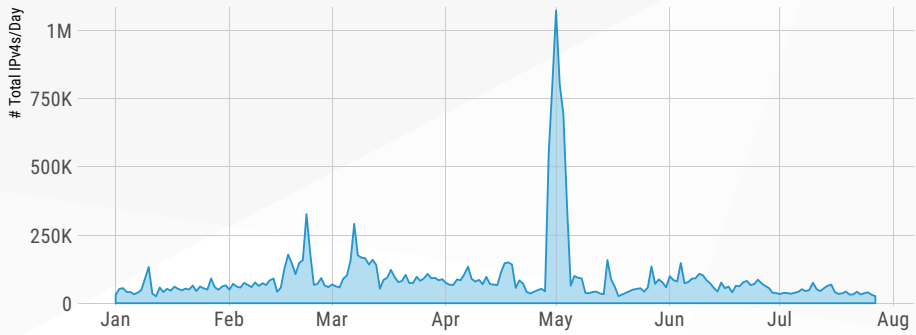
KEY FINDING: RDP OF DOOM

Since the Shadow Brokers' leak in April 2017, Rapid7 has been tracking the use of EternalBlue against systems in our honeypots. Over the past year, we have consistently seen a steady increase in activity targeting Microsoft's SMB protocol—and it's not subsiding. A potential side effect of realizing that there is far more SMB open to the internet is that adversaries have started becoming more interested in older protocols that we collectively thought would be long gone from modern networks, including Microsoft's Remote Desktop Protocol (RDP). While some adversaries use stolen credentials to gain access to systems, many of the access attempts we see still utilize brute force methods for gaining access.

Unlike the steadily increasing attacks against SMB, we see a consistent level of activity with RDP dotted by peaks. Sometimes these peaks are surprisingly high, such as the spike at over 1 million probes at the beginning of May. Brute force attacks are linked to recent attacks such as SamSam[6] ransomware, which has targeted the healthcare sector as well as state and local governments in past quarters. SamSam hit multiple healthcare organizations in Q2 and moving into Q3.

Figure 5: Daily Remote Desktop Protocol (RDP) Incidents Recorded by Project Heisenberg Honeypots

Weekly percentage is the percentage of incidents that week out of all incidents in Q1 2018



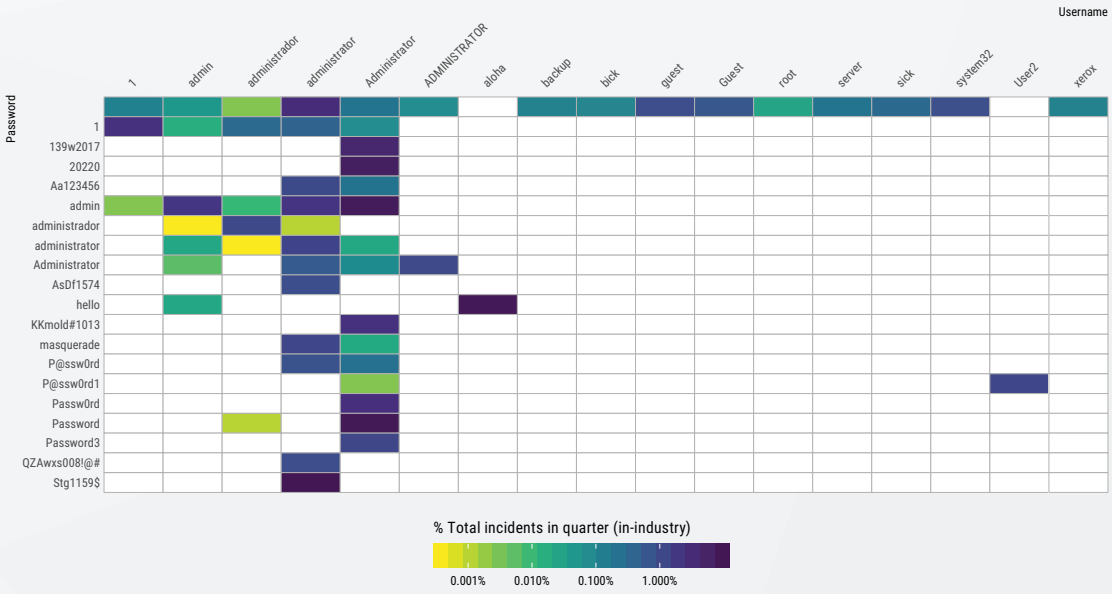
Source: Rapid7 Project Heisenberg & GreyNoise Intelligence

Although there are exploits available for RDP, many attackers prefer to leverage credentials to gain access to systems over RDP. Rapid7's Project Heisenberg keeps track of ways that we see attackers trying to gain access to systems, including the usernames and passwords that attackers use. When we focus in on RDP-specific password-guessing attempts, there are some interesting trends that are not seen across other authenticated protocols:

- **An emphasis on usernames with no passwords:** The majority of usernames that attackers tried against our systems had no password at all. This is a departure from what we have seen against other protocols, where attackers will try an empty password but follow it up with a variety of other potential default passwords. With RDP, we often only saw an empty password attempted.

Figure 6: Top Usernames and Passwords Attempted on RDP

Includes only the intersection of the top 20 usernames and top 20 passwords. Percentages calculated based on all observed username and password combinations.



Source: Rapid7 Heisenberg Cloud

[6] https://www.secureworks.com/research/samsam-ransomware-campaigns

Attackers have a long history of using backup servers both as a way to gain access to a network and also to obtain sensitive information that may be stored on an unsecured backup.

- **Targeting backups and other specific systems:** The top usernames attempted against RDP included things such as "backup" and "xerox," giving defenders some indication of what types of systems they are trying to gain access to. These are often systems that are easy for defenders to overlook. Attackers have a long history of using backup servers both as a way to gain access to a network and also to obtain sensitive information that may be stored on an unsecured backup.
- **Using specific passwords:** It is pretty common for us to see the top 20 passwords attempted include the defaults we have come to know and love (think "admin1234" and "abc123"). With RDP, however, many of the top passwords are specific strings that are not commonly used default passwords. We are still investigating whether these are passwords found in password dumps or are the defaults for a specific system the adversary is focusing on. However, monitoring which strings we see over time can help us understand what the adversary is targeting. If you're using these very common strings as your passwords, you've got to change them. Use the random password generator that came with your password management solution—you are using a password manager now, right?

KEY FINDING: PLANETARY-SCALE INTELLIGENCE

Rapid7's Project Heisenberg has over 150 honeypot nodes spread across the internet watching for signs of attacker activity and analyzing attacker behavior and methodology. If Q1 could be summed up as the "rebirth of amplification distributed denial of service (DDoS)[7] attacks," Q2 marks the rise of the cryptominer injectors—though that was not our adversaries' only goal.

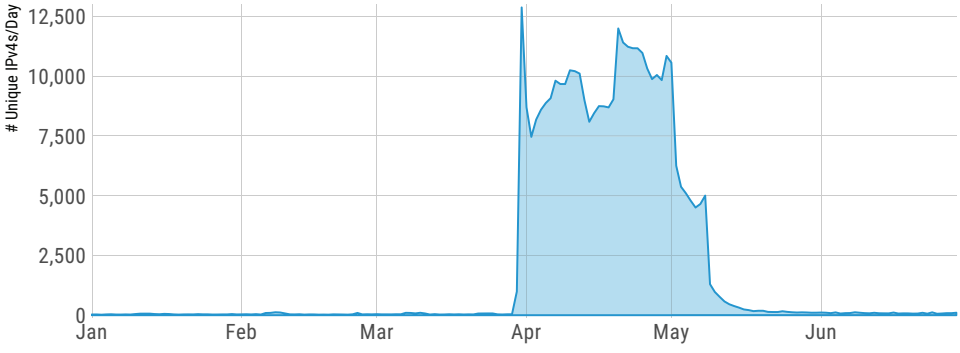
MikroTik Madness

April started with a campaign against—and, using—MikroTik[8] routers that lasted through mid-May (Figure 7). These devices are cheap, small, performant, and popular in many regions of the globe. They ship with a wide attack surface enabled by default (virtually every admin access port you can enumerate), do not force credential changes for deployment, and tend to be woefully ill-maintained. Campaigns against MikroTik devices generally cycle through default credentials and use well-known exploits. Using a recently patched critical vulnerability[9], a prolific, active campaign remotely steals credentials and turns these nodes into attacker tools with the vast majority of still-vulnerable devices (at report publication time) mining cryptocurrency via Coinhive[10] by injecting custom JavaScript into any web traffic that passes through a compromised MikroTik device. Over half of the 300,000 (Figure 8) exposed MikroTik devices on the internet have been seen participating in the mining.

If you use MikroTik equipment, it might be best to facilitate a project that cycles through each device and lays down a secure configuration that's fully patched, meaning changed credentials, minimal internal services exposed, and no services exposed to the internet-facing side. It is also vital to subscribe to MikroTik's support feeds and monitor MikroTik's download page[11] for new software updates. You should also consider setting up a Google alert[12] for "MikroTik" and a custom Google News category[13] subscription to be informed of breaking news for new MikroTik vulnerabilities and attacks/campaigns.

Q2 marks the rise of the cryptominer injectors—though that was not our adversaries' only goal.

Figure 7: MikroTik Worm and Compromise Attempt Activity



Source: Rapid7 Project Heisenberg & GreyNoise Intelligence

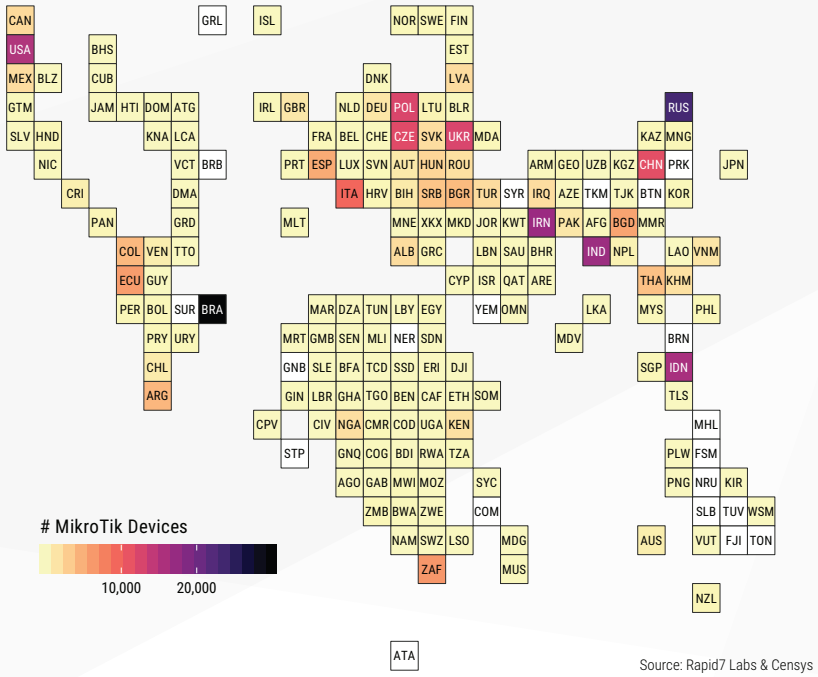
7 https://blog.rapid7.com/2018/02/27/the-flip-side-of-memcrashed/
8 https://mikrotik.com/
9 https://www.cvedetails.com/cve/CVE-2018-7445/
10 https://coinhive.com/
11 https://mikrotik.com/download
12 https://www.google.com/alerts
13 https://news.google.com/search?q=mikrotik

VPNFilter Redux

If you're thinking you saw the MikroTik brand in headlines more than once this past quarter, you'd be right. MikroTik made an appearance in the list of router brands targeted by the VPNFilter[14] malware campaign, which has compromised over half a million devices. On the plus side, this means attacker groups are vying for control over each other's "stash." On the downside, it is not hyperbole to suggest that the the number of compromised routers, cameras, set-top boxes, and other parts of the IoT-verse is in the millions. Collectively, that's quite an arsenal, but (thankfully?) the individual components are mostly focused on nondestructive tasks such as cryptomining. However, as the U.S. Federal Bureau of Investigation (FBI) itself notes[15]:

Figure 8: MikroTik Device Tile Grid Distribution

Country distribution of all MikroTik devices (over 300K identified in the July 2018 scans)



Source: Rapid7 Labs & Censys

> "VPNFilter is able to render small office and home office routers inoperable. The malware can potentially also collect information passing through the router. Detection and analysis of the malware's network activity is complicated by its use of encryption and [sic] misattributable networks."

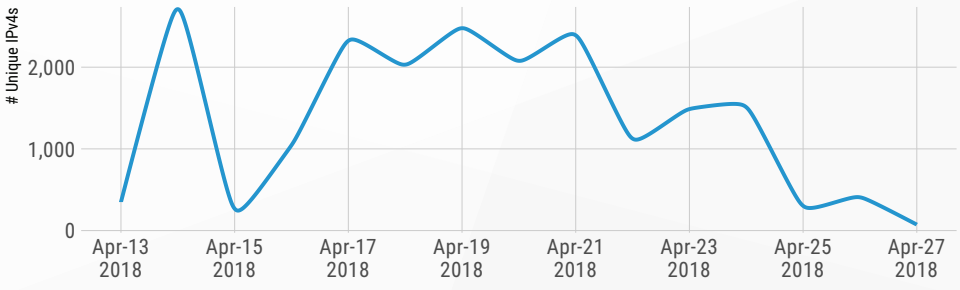
This means the VPNFilter threat should not be taken lightly. The nodes pose a threat to both the owners and users of these devices and are easily repurposed by attackers to launch attacks against other users, networks, and organizations.

Drupal Downer

While this was going on, other attackers focused their attention on web servers running Drupal (Figure 9) during the latest round of Drupa[l]geddon[16]. Attackers compromise sites for many reasons, including credential theft, using systems with a neutral or benign reputation as command-and-control nodes, spam spewing servers, and denial of service (DoS) attack nodes. A more modern use of vulnerable systems is to install cryptominers on them. Digital currency valuations are always in flux, but they are still prized targets for attackers, especially after criminal organizations discovered that it takes quite a bit of hands-on helpdesk and support effort to make ransomware profitable. The key to keeping Drupal safe is to minimize your use of non-core server modules and keep an eye out for patch releases and unusual activity in your weblogs.

Figure 9: Drupalgeddon—Unique IPv4s Per Day

We looked back to the first of April and didn't see any of the tell-tale attack signs until April 13th



NOTE: Heisenberg network redeployment occurred on April 15
Source: Rapid7 Project Heisenberg & GreyNoise Intelligence

14 https://blog.rapid7.com/2018/06/07/vpnfilter-potential-reach/

15 https://www.ic3.gov/media/2018/180525.aspx

16 Attackers are not known for their proficiency in spelling, and the first round of Drupal attacks were tagged by them without the "l".

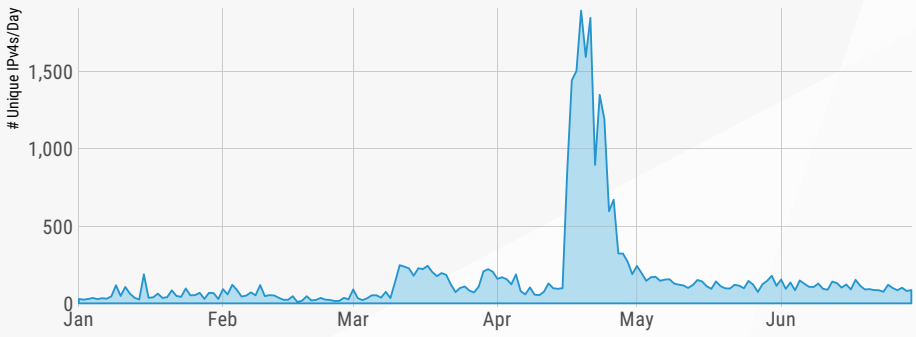
Whacking WebLogic

April also brought with it an attempt to use CVE-2017-10271[17] to enlist vulnerable WebLogic servers into the ranks of zombie cryptocurrency miners. As you can see in Figure 10, the campaign was brief, but it should serve as yet another reminder to make sure your Java-based services are well-configured and patched as soon as possible.

I Want ~~My~~ Your ADB (Android Debug Bridge)

To paraphrase Dire Straits, "Look at those hackers / that's the way you do it / do your crypomining over ADB." We owe a "hat tip" to Kevin Beaumont, who started a collaboration[18] on this (continuing) incident in early June. It turns out tons of Android devices—mostly internet set-top boxes and pirate TV boxes—ship with the Android Debug Bridge[19] service enabled (generally on port 5555). Some clever attackers noticed this and had the equally clever idea of turning these glowing-rectangle controllers into—you guessed it!—**cryptominers**, starting back in February (Figure 11).

Figure 10: WebLogic Cryptominer Injection Campaign



Source: Rapid7 Project Heisenberg & GreyNoise Intelligence

To add to the intrigue, a fair number of port 5555 attack sources and targets are on mobile networks. Rapid7 Labs has been noticing an increased level of general attacks and probes coming from these usually opaque parts of the internet, and we're keeping an eye out on both the cryptominer campaigns and the use of mobile network nodes in other campaigns to determine whether there's a more determined pattern of attackers enlisting these mobile, transient nodes in their bot armies.

Rounding Out the Corners

To close out our planetary view of attacker activity for the quarter, we've summarized four additional attack groups in Figure 12 that either had interesting/foreboding patterns or were part of views we've been tracking in our Threat Reports (note that the "dips" your eye will likely focus on in March and May are due to the redeployment of our entire honeypot network):

Figure 11: Android Debugger Service Cryptominer Injection Campaign

Source: Rapid7 Project Heisenberg & GreyNoise Intelligence

- Probes for active Bitcoin nodes and campaigns against these nodes are definitely spiking, and you should make sure to tune in to the Q3 Threat Report, as there are already signs of even broader-scale activity. If you run a bitcoin node, make sure the software is from a trusted source and at current patch levels. Try not to run anything else on these nodes, if at all possible.
- General probes and attacks for all manner of HTTP/HTTPS web-based services are at levels not seen before this year. We will reiterate our guidance to monitor your logs for unusual activity, keep your systems and servers patched, and issue further guidance to ensure security is a part of each phase in your application development lifecycle.

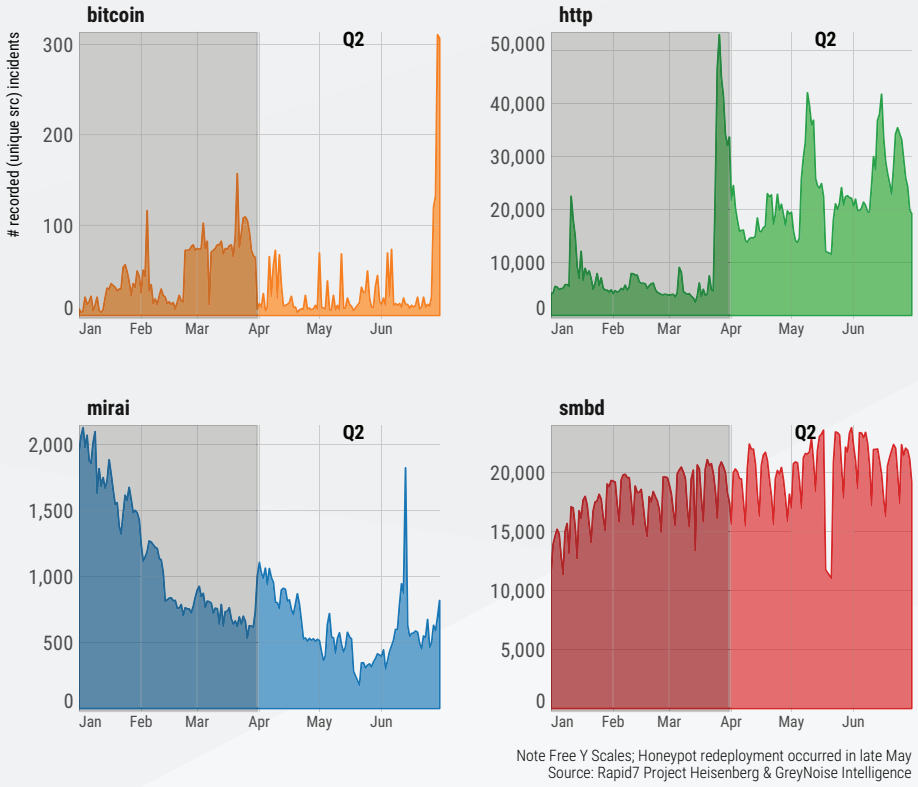
17 https://www.rapid7.com/db/vulnerabilities/oracle-weblogic-cve-2017-10271

18 https://doublepulsar.com/root-bridge-how-thousands-of-internet-connected-android-devices-now-have-no-security-and-are-b46a68cb0f20

19 https://developer.android.com/studio/command-line/adb

Figure 12: Inbound Incident Classification Activity by Target Service

Q2 saw increased attacker focus on Bitcoin, numerous flavors of HTTP attacks, the start of an uptick in Mirai and a levelling-off of SMB



Note Free Y Scales; Honeypot redeployment occurred in late May
Source: Rapid7 Project Heisenberg & GreyNoise Intelligence

- Mirai chatter activity has spiked, and the baseline level is increasing. Some of this is due to existing nodes searching for internet-enabled devices that have had recent vulnerability announcements. We'll cover more of Mirai in our Q3 report, but note here that now would be a great time to rethink how you configure, manage and, expose your cameras, doorbells, and security systems. Organizations should work with their risk management teams to ensure they have the level of DoS protection that meets their risk appetite. Mirai and the refresh of amplification DoS inventories that we noticed in Q1 have the potential to inflict serious damage, even under the best of mitigation services.
- Finally, let's take a look at this quarter's update on malicious activity targeting Microsoft protocols, generally associated with the Shadow Brokers exploits from last year. The "**smbd**" label in Figure 12 is largely made up of attempts to use EternalBlue exploits to acquire new nodes. Malicious activity is beginning to level off in general, but we'll be watching to see whether this is an indicator of a shift in attacker focus or just the dog days of summer taking their toll on the 9-to-5 attackers.

CONCLUSIONS

Overall, Q2 of 2018 served as a return to expected patterns of activity, with adversaries focusing on the sectors and data types that they have known and loved for years: financial data, customer information, and sensitive information that can be used in ways only limited by the attacker's imagination. Cryptomining is becoming a time-honored tradition among actors as well, as quarter after quarter we see an increase in cryptominers on systems, as well as new bot-based campaigns such as the recent MikroTik, WebLogic, and ADB activities.

Remote access reigns supreme both for stealing information and mining cryptocurrency. Credential theft, credential dumping, and brute force tactics all work for gaining access to systems. Monitoring for brute force activity, suspicious multi-country authentication, and multi-organization authentication helps to identify this type of activity, and implementing multi-factor authentication and monitoring for leaked credentials can help organizations actively protect themselves from these threats.

Understanding exposures is another critical aspect to combating the threats we see continuing quarter after quarter. Externally exposed RDP—even if it is just exposed for a short period of time—can have a devastating impact on an organization, as we saw with several of the RDP-enabled ransomware attacks in Q2. Exposure may not just impact your own organization's traditional IT infrastructure, but it can also mean your embedded systems, including cameras, doorbells, and motion sensors, are being added to botnets used to carry out additional attacks while zapping your own resources. Knowledge of threats, knowledge of your own environment, and an active approach to remediating threats and vulnerabilities will go a long way toward keeping you and your network above the fray.

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 second 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 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
- 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.

EVENT	DESCRIPTION
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.
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 powers the practice of SecOps by delivering shared visibility, analytics, and automation that unites security, IT, and DevOps teams. The Rapid7 Insight platform empowers these teams to jointly manage and reduce risk, detect and contain attackers, and analyze and optimize operations. Rapid7 technology, services, and research drive vulnerability management, application security, incident detection and response, and log management for organizations around the globe. To learn more about Rapid7 or get involved in our threat research, visit www.rapid7.com.

QUESTIONS?

Email us at research@rapid7.com