Threat Landscape Trends – Q2 2020

A look at the cyber security trends from the second quarter of 2020.

As the first half of the year drew to a close, we took a look through telemetry from our vast range of data sources and selected some of the trends that stood out from April, May, and June 2020.

From a resurgence in cryptojacking activity to the return of a major malware distribution platform, let's take a quick look at the trends that shaped the cyber security threat landscape in the second quarter of 2020.

Cryptojacking

After a sharp decline in cryptojacking following the shutdown of browser-based mining script maker CoinHive in March 2019, the second quarter of 2020 saw a resurgence in activity. Browser-based cryptojacking events blocked by Symantec saw a 163 percent increase in Q2 2020 compared to the previous quarter. This spike in activity coincides with an increase in the value of cryptocurrencies, including Bitcoin and Monero, which are two currencies often mined by browser-based coinminers.

For more information on cryptojacking, read our blog:

Cryptojacking: A Modern Cash Cow

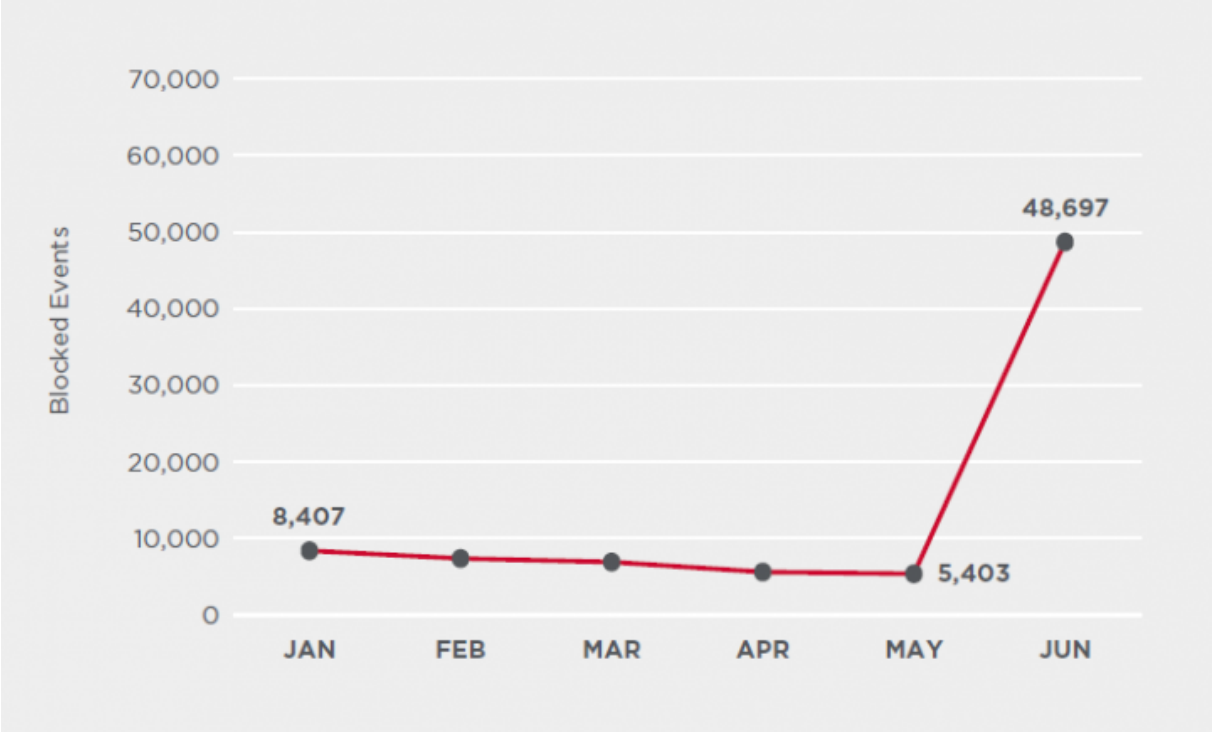

Figure 1. Browser-based cryptojacking events blocked by Symantec were up 163 percent in Q2

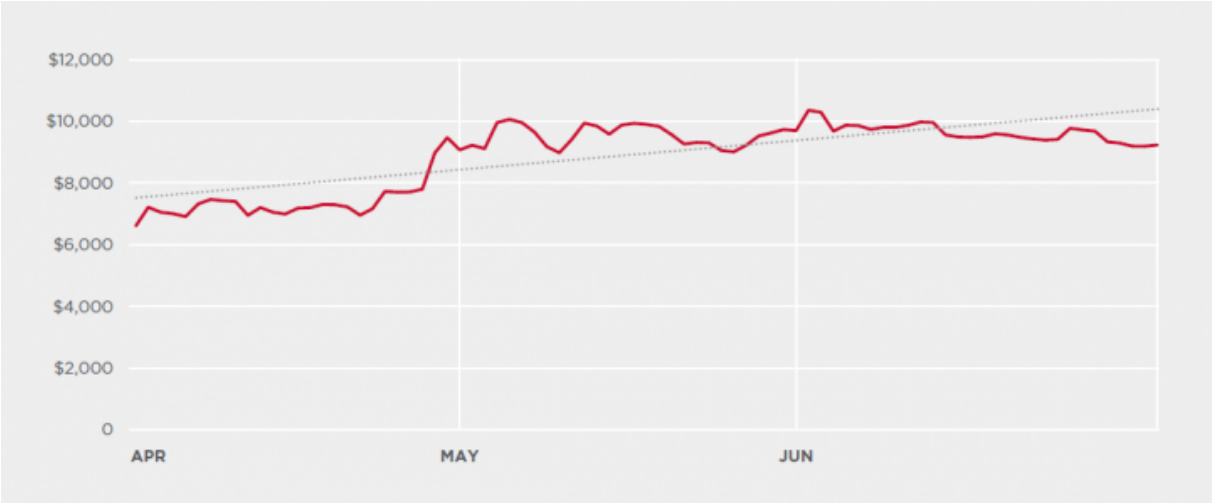

Figure 2. Bitcoin price over Q2

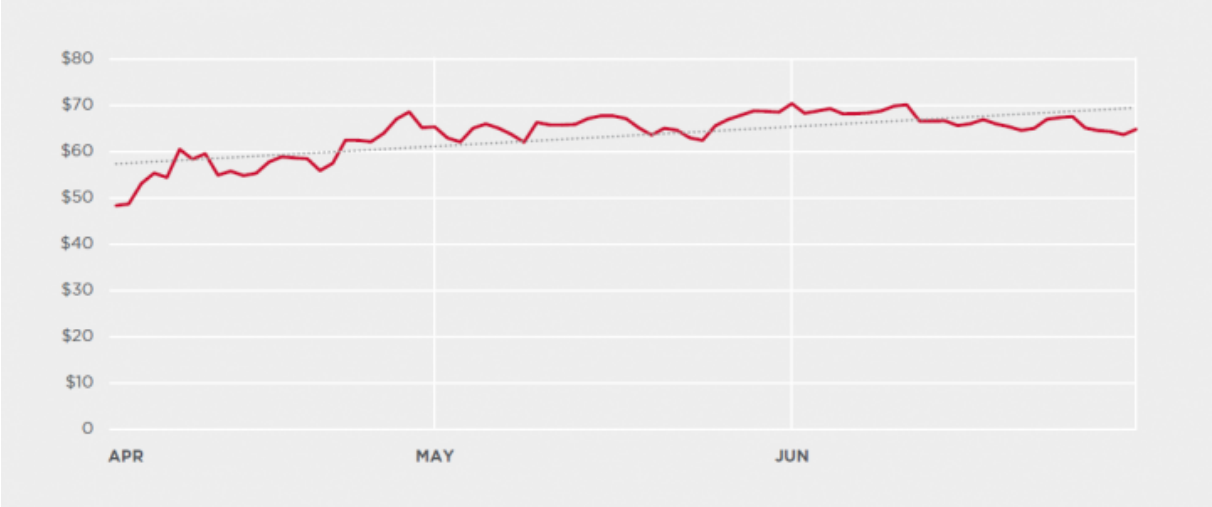

Figure 3. Monero price over Q2

Malware Increases as Lockdown Restrictions Ease

As countries around the world began easing COVID-19 lockdown restrictions, malware distributors also resumed working at full capacity. May and June saw a significant increase in the number of malware attacks blocked by Symantec, a division of Broadcom (NASDAQ: AVGO). In total, Symantec blocked over 60 million infection attempts in the second quarter of 2020, which represents a 74.6 percent increase over the previous quarter.

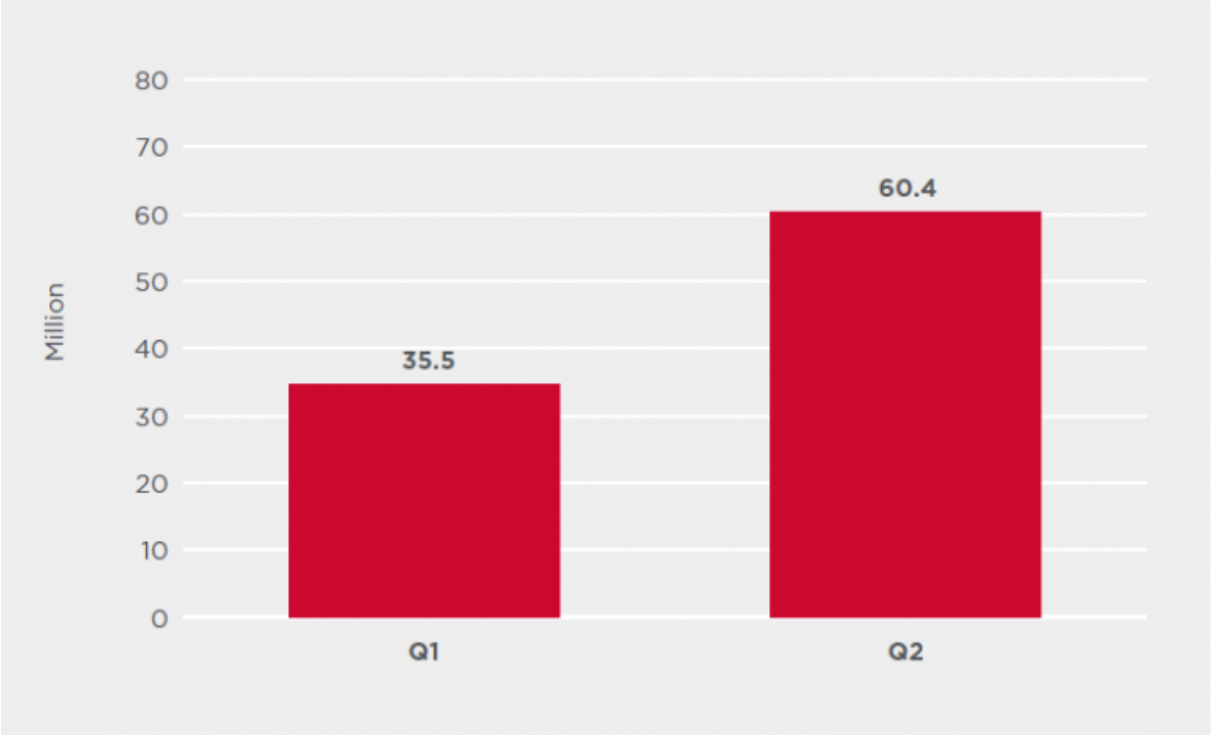

Figure 4. Symantec blocked over 60 million malware infection attempts in Q2 2020, a 74.6% increase over Q1

Emotet

For over a year, the Emotet botnet (Trojan.Emotet) has been subdued, with two long periods of inactivity: Between May and September 2019 and again between February and July 2020. This drop-off in activity is reflected in Symantec's detections of new Emotet infections during this period. However, while activity for Q2 remained nominal, the botnet ramped up its activity in early Q3. Emotet's return is a source of concern, since it is a major malware distribution platform.

For more information on Emotet, read our blog:

The Evolution of Emotet: From Banking Trojan to Threat Distributor

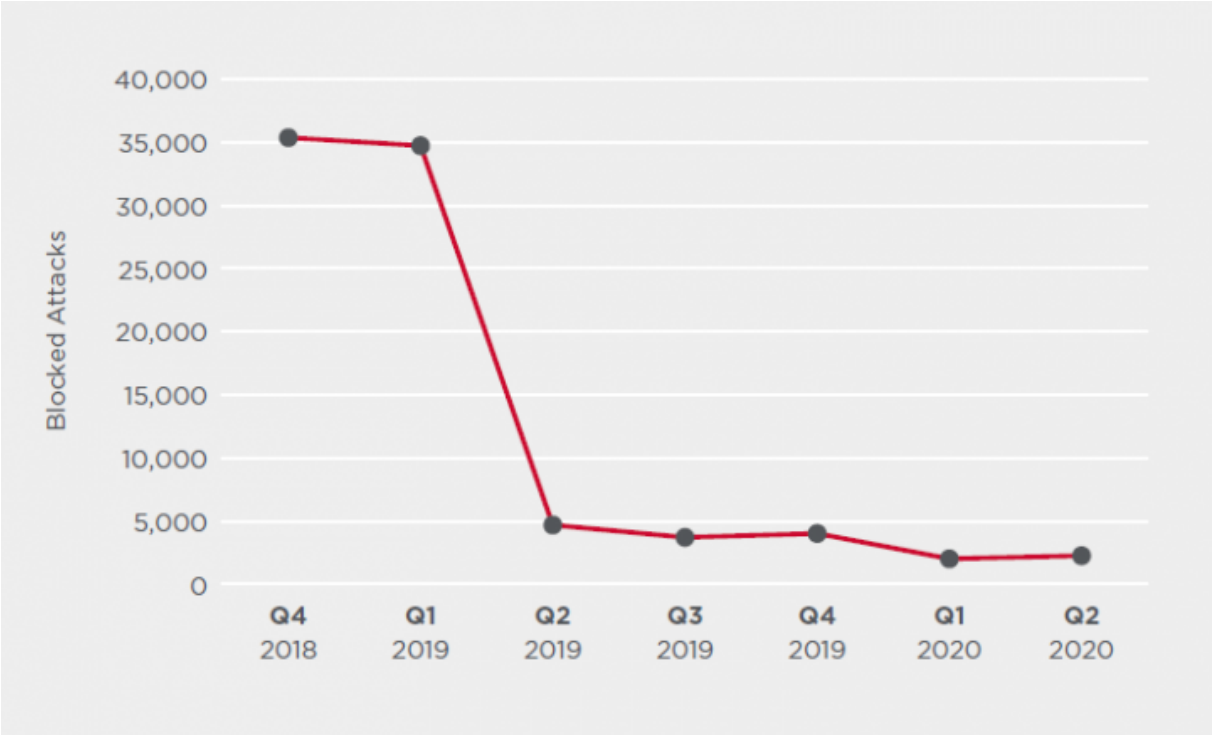

Figure 5. The Emotet botnet was subdued in Q2 but since beginning of Q3 has ramped up activity

Sodinokibi

There was an increase in attacks using the targeted Sodinokibi ransomware (Ransom.Sodinokibi), also known as REvil, in the second quarter of 2020. Following a lull in March, activity began to increase again in April. By the end of Q2, Sodinokibi activity was up by over 630 percent, compared to the end of Q1. This ties in with research from Symantec in June which revealed a Sodinokibi campaign in which the attackers were using the Cobalt Strike commodity malware to deliver Sodinokibi to victims in the healthcare, services, and food sectors.

For additional information on Sodinokibi, read our blog:

Sodinokibi: Ransomware Attackers also Scanning for PoS Software, Leveraging Cobalt Strike

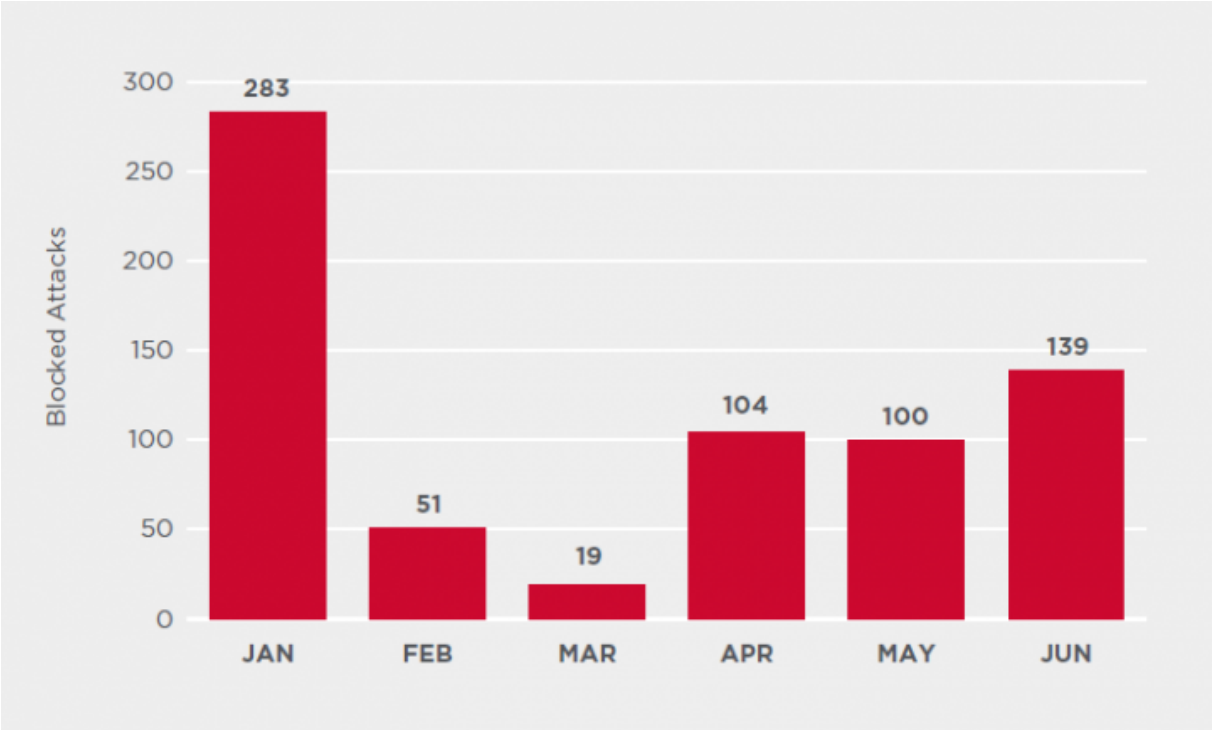

Figure 6. Sodinokibi activity at the end of Q2 was up by over 630 percent, compared to end of Q1

Cobalt Strike

A growing number of attacks in recent months have involved the use of Cobalt Strike (Backdoor.Cobalt), a multipurpose commodity malware available for purchase, most notably used in the WastedLocker (Ransom.WastedLocker) targeted ransomware attacks. Reflecting this trend, detections of intrusions involving confirmed Cobalt Strike usage are up significantly in the past two quarters. In many cases, Cobalt Strike is blocked by other detection technologies and signatures, meaning the true number of attacks involving this malware may be significantly higher.

For more information on WastedLocker and its use of Cobalt Strike, read our blog:

WastedLocker: Symantec Identifies Wave of Attacks Against U.S. Organizations

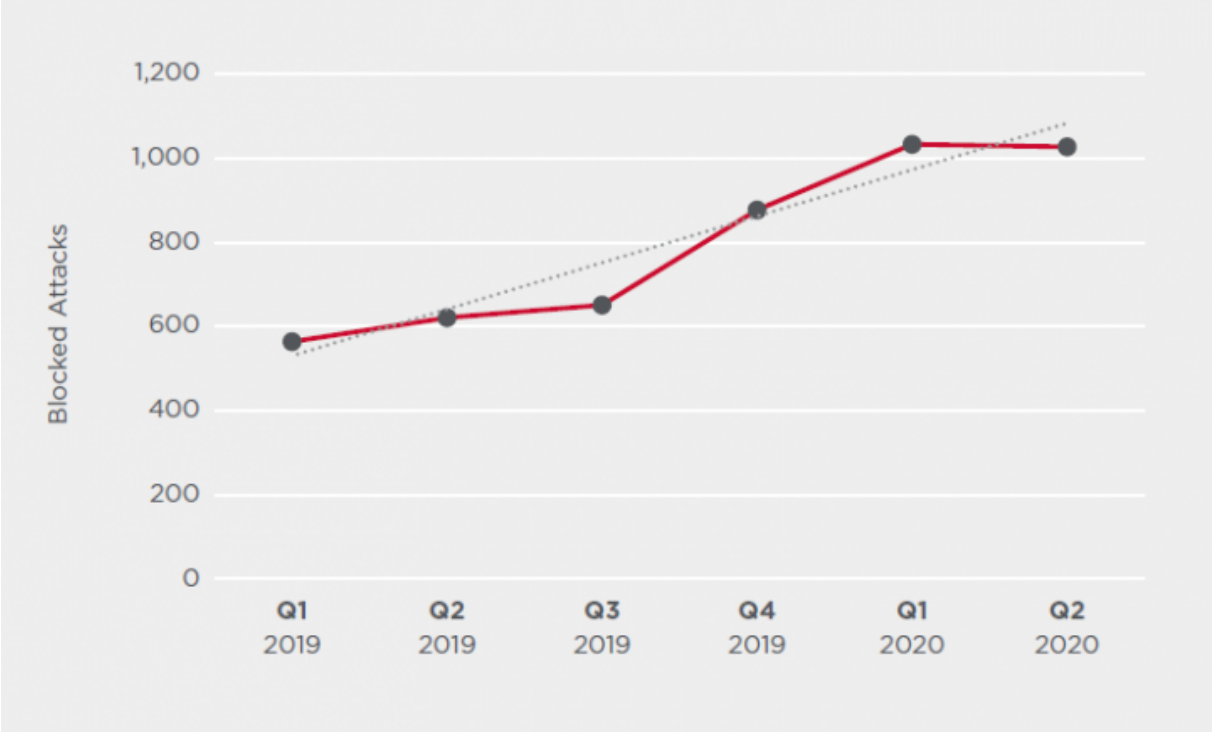

Figure 7. Detections of intrusions involving confirmed Cobalt Strike usage are up significantly in the past two quarters

Lokibot

The Lokibot information-stealing malware (Infostealer.Lokibot) saw a spike in activity in June, with blocked attacks increasing by almost 800 percent over the previous month. If this increased activity continues, Q3 could see Lokibot match or surpass activity seen in Q1.

Lokibot, one of today's most prevalent information-stealing threats, is often distributed via spam campaigns. Symantec recently began monitoring two new spam campaigns spreading Lokibot and targeting medium and large businesses around the world. One campaign involves the impersonation of a Saudi company specializing in industrial services and another impersonates a large shipping firm.

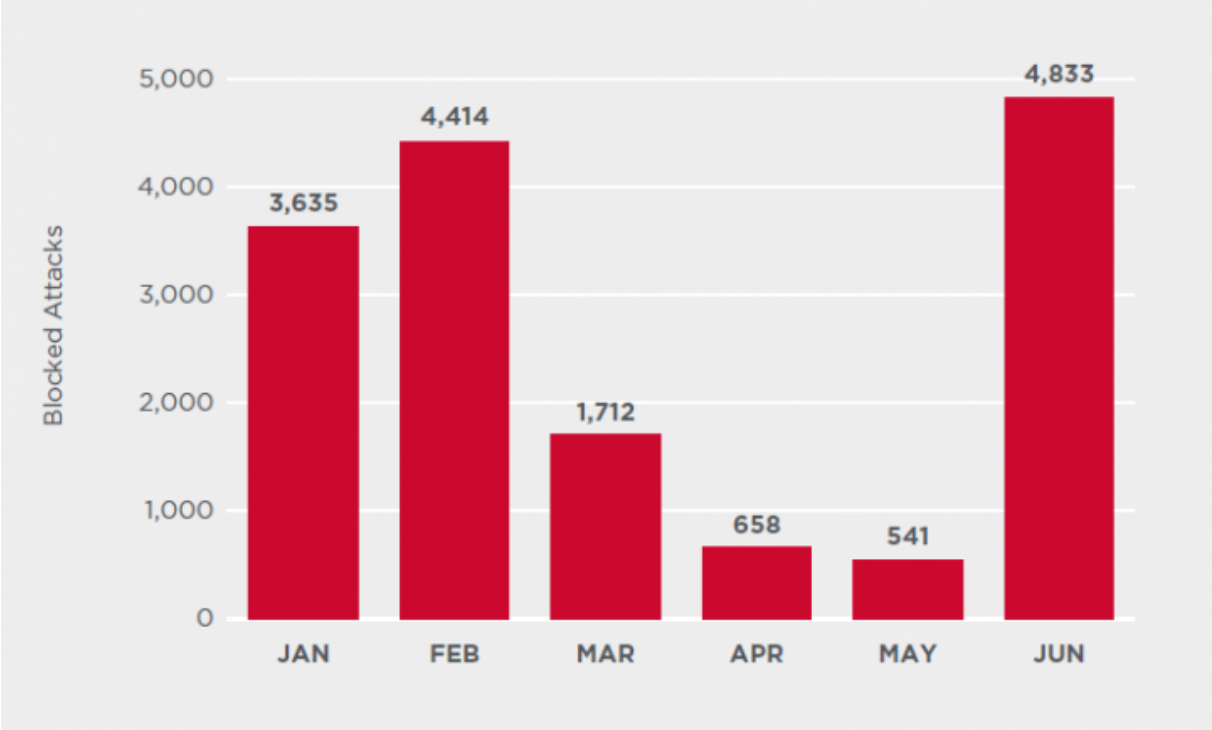

Figure 8. Blocked Lokibot attacks in June increased by almost 800 percent over the previous month

IoT Attacks Decline but Risk Remains

The number of attacks against Symantec Internet of Things (IoT) honeypots* per day was down 12 percent in Q2 compared to Q1 2020. However, Q2 2020 still saw a greater number of attacks (14 percent more) compared to Q4 2019. While the numbers may be down, the risk of attack against internet-connected devices still remains high, as highlighted by a recent alert jointly released by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the UK's National Cyber Security Centre (NCSC) warning QNAP NAS device owners to update their devices in case QSnatch malware attacks restart.

The number of unique IP addresses performing IoT attacks also fell in Q2, down 19 percent over the previous quarter.

**Symantec's IoT honeypots emulate protocols used by virtually all IoT devices, such as routers, connected cameras, digital video recorders, and so on.*

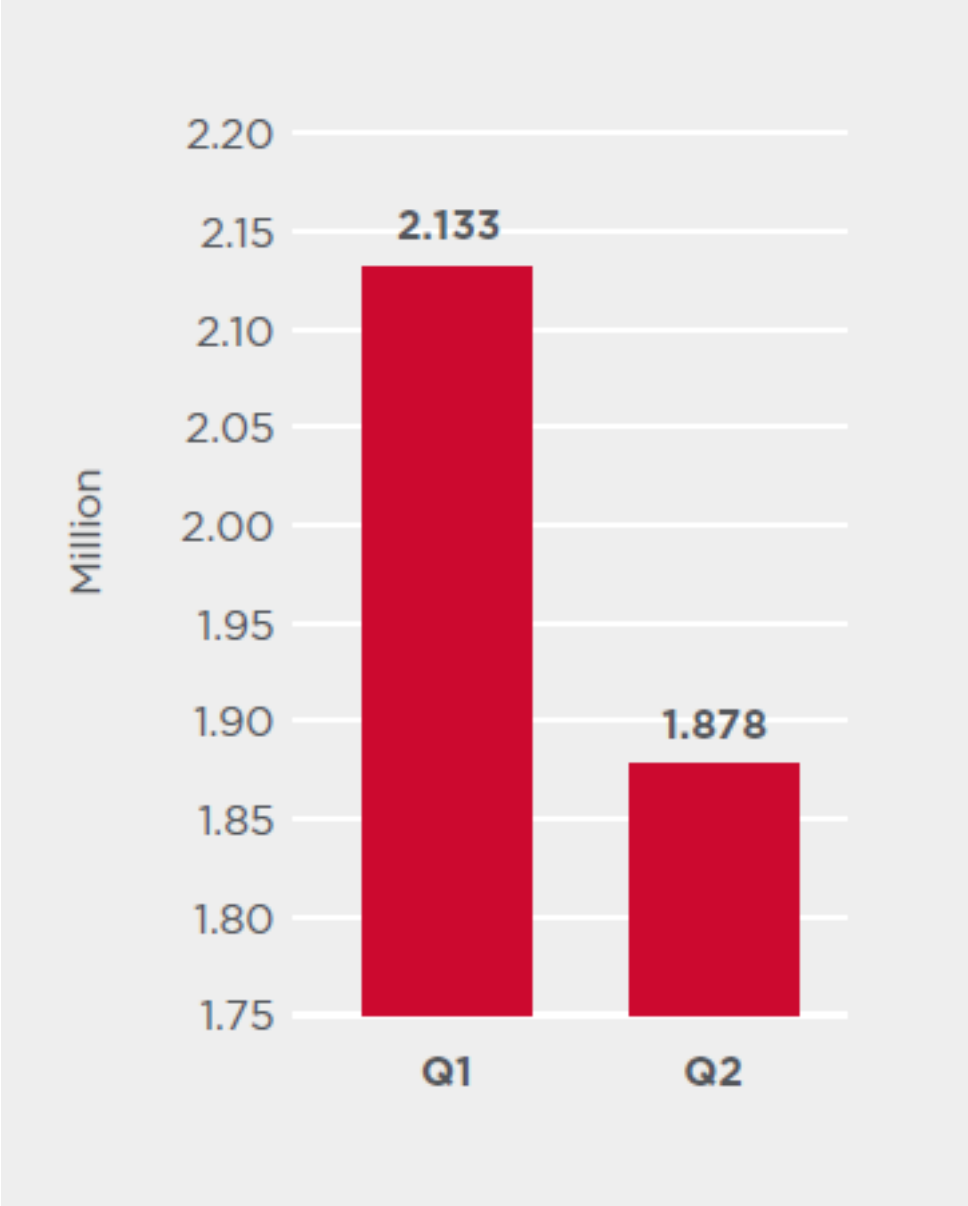

Figure 9. Average number of IoT attacks per day

Top User Names and Passwords

The top ten user names and passwords used in attacks on IoT devices. Most of the credentials used by attackers are default or easily guessable.

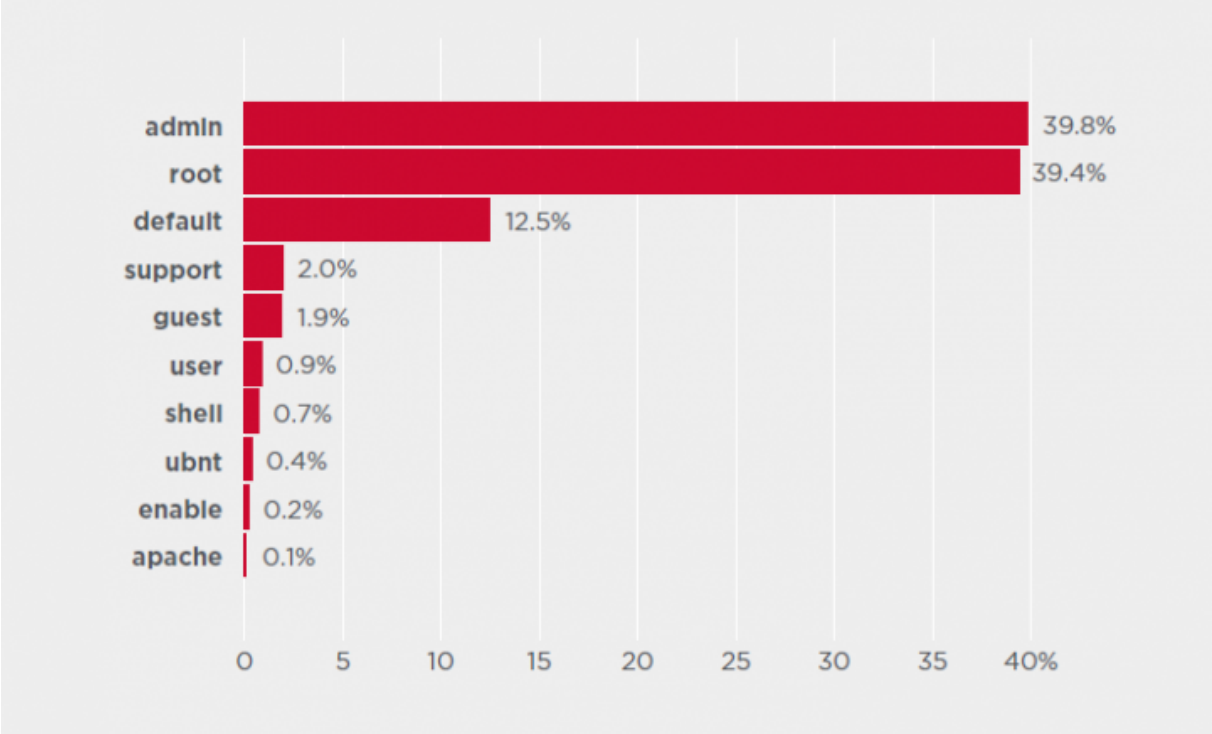

Figure 10. Top 10 user names used in IoT attacks

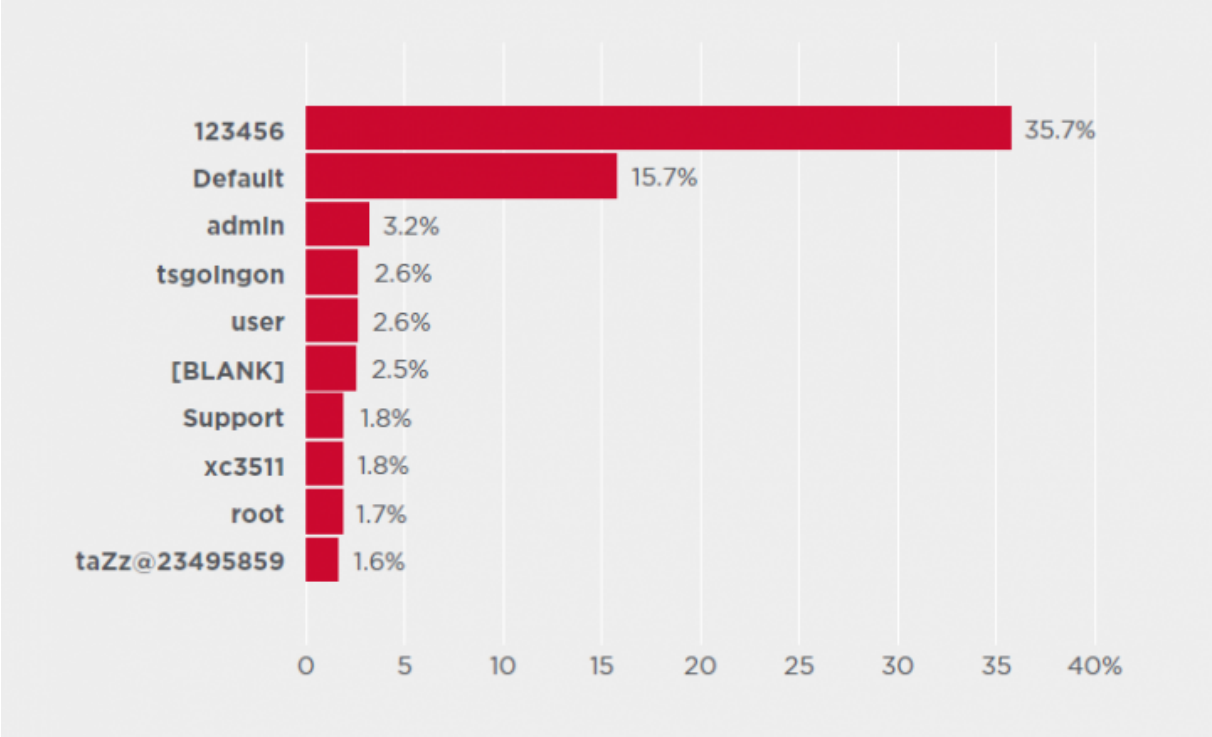

Figure 11. Top 10 passwords used in IoT attacks

Attack Origination

The largest amount of attacks originated from IP addresses located in the U.S. followed by China, Taiwan, Brazil, and Russia. Since attacks are carried out by botnets of infected IoT devices, these regions have the highest number of infected IoT devices.

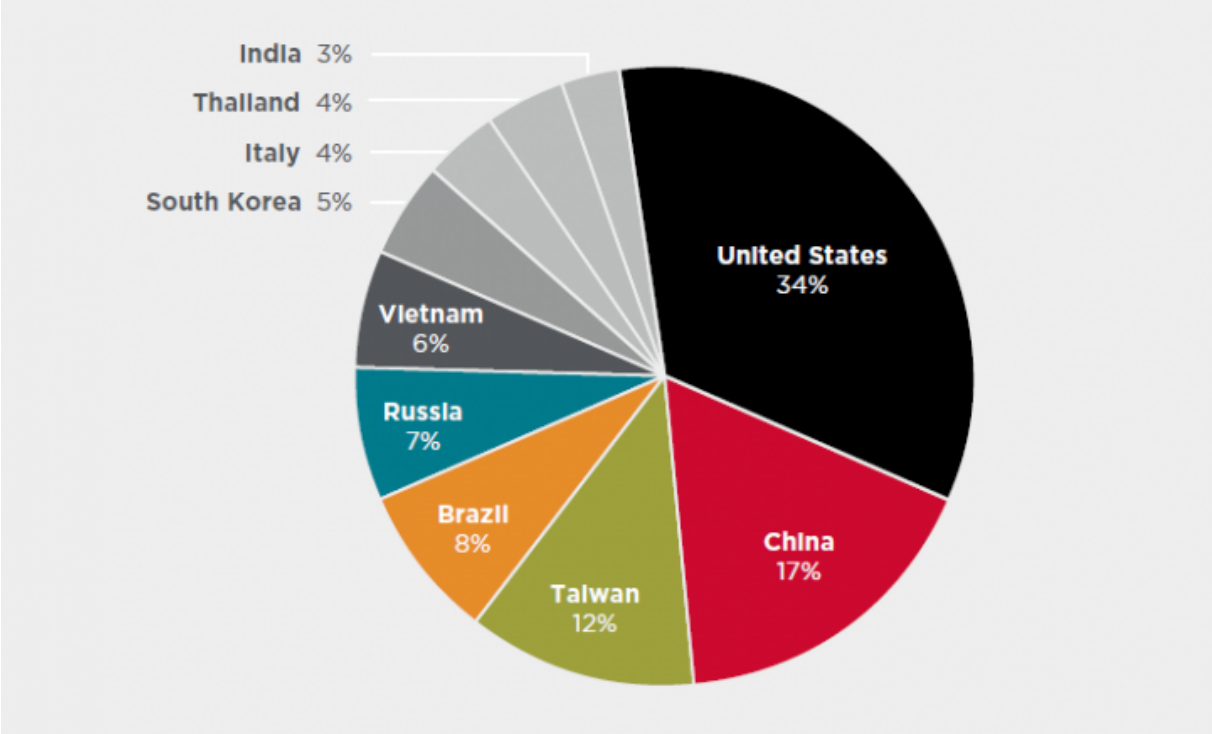

Figure 12. Majority of IoT attacks originated from IP addresses in the U.S. followed by China

For the latest insights on threat intelligence visit Symantec Enterprise Blog/Threat Intelligence.