

2022 Small Business Cybersecurity Report



Cybersecurity is a Persistent and Complex Problem

Business decision makers need to understand the threat landscape and the risks it poses. This first annual **Comcast Business Small Business Cybersecurity Report** reviews anonymized threat data gathered from our Comcast Business SecurityEdge™ service from July 2021 to June 2022, as well as security insights from our partner Akamai. The report offers a window into threats our small and medium-sized business (SMB) customers face on a daily basis and how our service helps protect them from these cyberthreats.



COMMON INTERNET THREATS



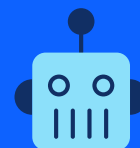
Phishing Attacks are Easy to Launch

Phishing remains a common cyberattack method because threat actors use it to prey on the fear, trust and curiosity of everyday users. Attackers constantly change and refine tactics to trick users. They can buy prebuilt kits that make it easier for even inexperienced hackers to deploy large-scale attacks.



Phishing is Used to Steal Information and Introduce Ransomware

Hackers use phishing to trick users. They draw users to websites containing malicious software that can be downloaded to computers to locate and encrypt data. Once systems are encrypted, hackers demand ransom to provide a decryption key. They can also steal credentials or other valuable data, damage or disrupt devices, or gain unauthorized access to a network.



Bots Can Propagate on Their Own and Support Other Exploits

Phishing also can be used to secretly install “bot” software on computers. Once installed, bots can be remotely controlled and even installed in other computers. Networks of bots can find and steal valuable information, launch Distributed Denial of Service (DDoS) attacks, and perform other malicious activities.

Executive Summary

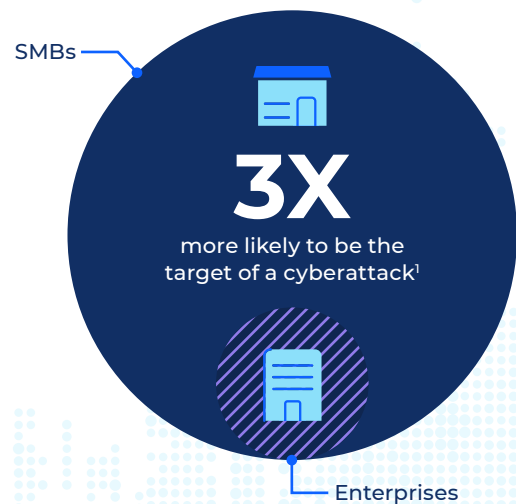
The security landscape remains challenging. So far in 2022, we have seen a number of high-profile cyberattacks against organizations such as Nvidia, News Corp, Microsoft, Samsung, and the Red Cross. While attacks against large organizations usually grab headlines, SMBs also face cybersecurity risks and attacks.

Attackers don't discriminate by size. Like their larger counterparts, SMBs have valuable data and financial resources that threat actors often target. Besides, SMBs far outnumber large organizations and often lack sufficient cybersecurity measures and resources to manage their risk. Furthermore, attackers seem to target SMBs more often than enterprises; a recent report estimates that users at companies with fewer than 100 employees are [three times more](#) likely to experience a cyberattack.

More than half of SMBs (58%) have suffered at least one security incident, according to the Identity Theft Resource Center's [2021 Business Aftermath Report](#). Data breaches at small companies in 2020 and 2021 [increased 152%](#) compared to the two prior years, according to RiskRecon, a MasterCard company. Larger companies suffered half the number of breaches in the same time period. A [survey of small businesses conducted by CNBC](#) in April 2022 found that 38% of SMBs worried about suffering a cyberattack in the next 12 months.

SMBs ARE MORE FREQUENT TARGETS OF CYBERATTACKS

than larger companies



58%  152% increase in data breaches at SMBs in 2020 and 2021³

Of SMBs have suffered at least one security incident²

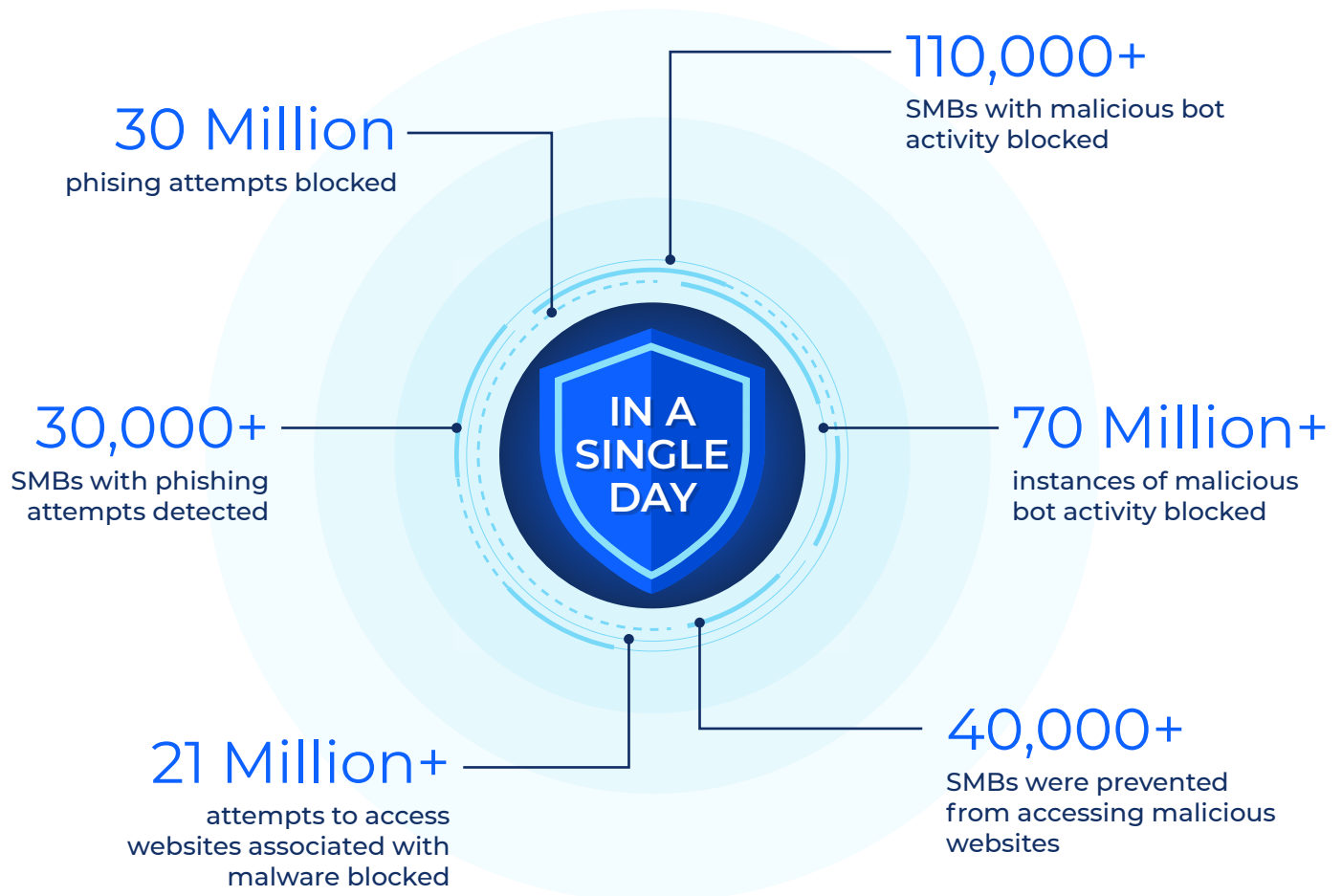
38%

Of SMBs worried about suffering a cyberattack in the next 12 months⁴

1. **Forbes:** "Small Businesses Are More Frequent Targets Of Cyberattacks Than Larger Companies: New Report"
2. **The Identity Theft Resource Center:** "Inaugural 2021 Business Aftermath Report Shows the Impacts Identity Crimes Have on Small Businesses"
3. **Tripwire:** "Weak Cybersecurity is taking a toll on Small Businesses"
4. **CNBC:** "America's small businesses aren't ready for a cyberattack"

Threat Data Insights

Over the 12 months from July 2021 to June 2022, Comcast Business SecurityEdge™ helped protect our SMB customers from various cyberthreats. Here are some highlights:



Source: Comcast Business SecurityEdge™/Akamai Research



Akamai collects data on Internet traffic across the full spectrum of industries and geographies. Data from the most recent quarter (Q2 2022) showed:



More than 12% of devices found in typical businesses showed evidence of exposure

to threats such as malware, phishing, or bots at least once.



Financial & high-tech brands were the most targeted by phishing scams

as they suffered 41% and 36% of attempts, respectively.



The use of one phishing kit extended to more than 500 web domains

which included financial institutions.

Business Impact

Profit is a big motivator for cyberattacks

Hackers make money by selling stolen credentials, customer data, financial information, and intellectual property. Attacks can compromise internal systems, damage infrastructure and permanently destroy data. A small or midsize company that suffers a cyberattack may not be able to afford all of the expenses it incurs to recover from it.

According to the [Identity Theft Resource Center](#), 44% of SMBs paid \$250,000 to \$400,000 for recovery costs, and 16% paid up to \$1 million. And according to the [Hiscox Cyber Readiness Report 2021](#), one in six firms attacked in the past year struggled to survive.

44%

Of SMBs paid \$250,000 to \$400,000 for recovery costs⁵

16%

Of SMBs paid up to \$1 million for recovery costs⁵

1 IN 6

Firms attacked in the past year struggled to survive⁶

5. **The Identity Theft Resource Center:** "2021 Business Aftermath Report: Infographic with key findings"

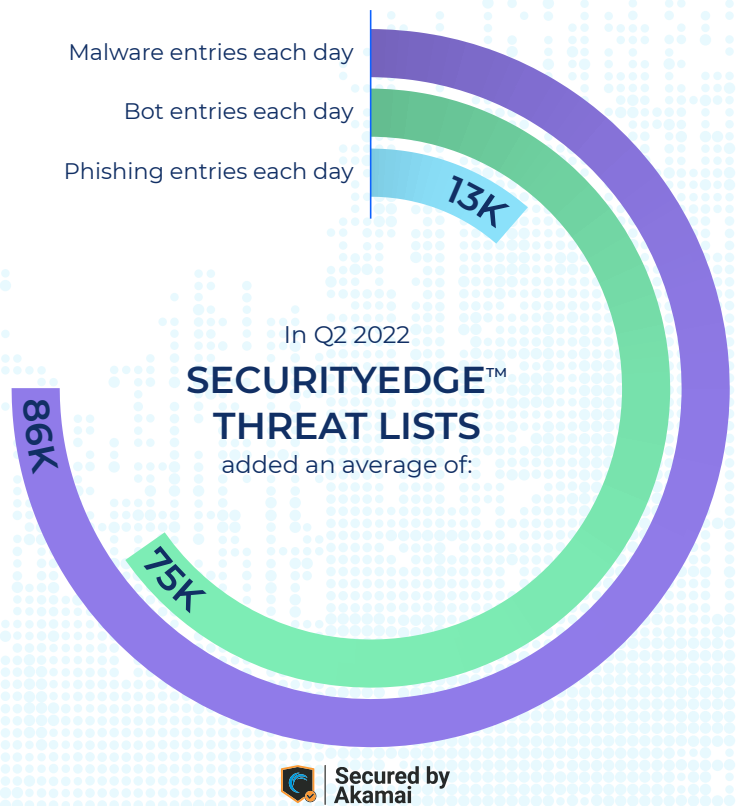
6. **Hiscox:** "Hiscox Cyber Readiness Report2021: Don't let cyber be a game of chance."

Comcast Business SecurityEdge™

Comcast Business SecurityEdge™ helps protect users and all their connected devices against threats such as malware, ransomware, phishing and botnets with advanced global threat intelligence powered by Akamai which is

updated every five minutes.

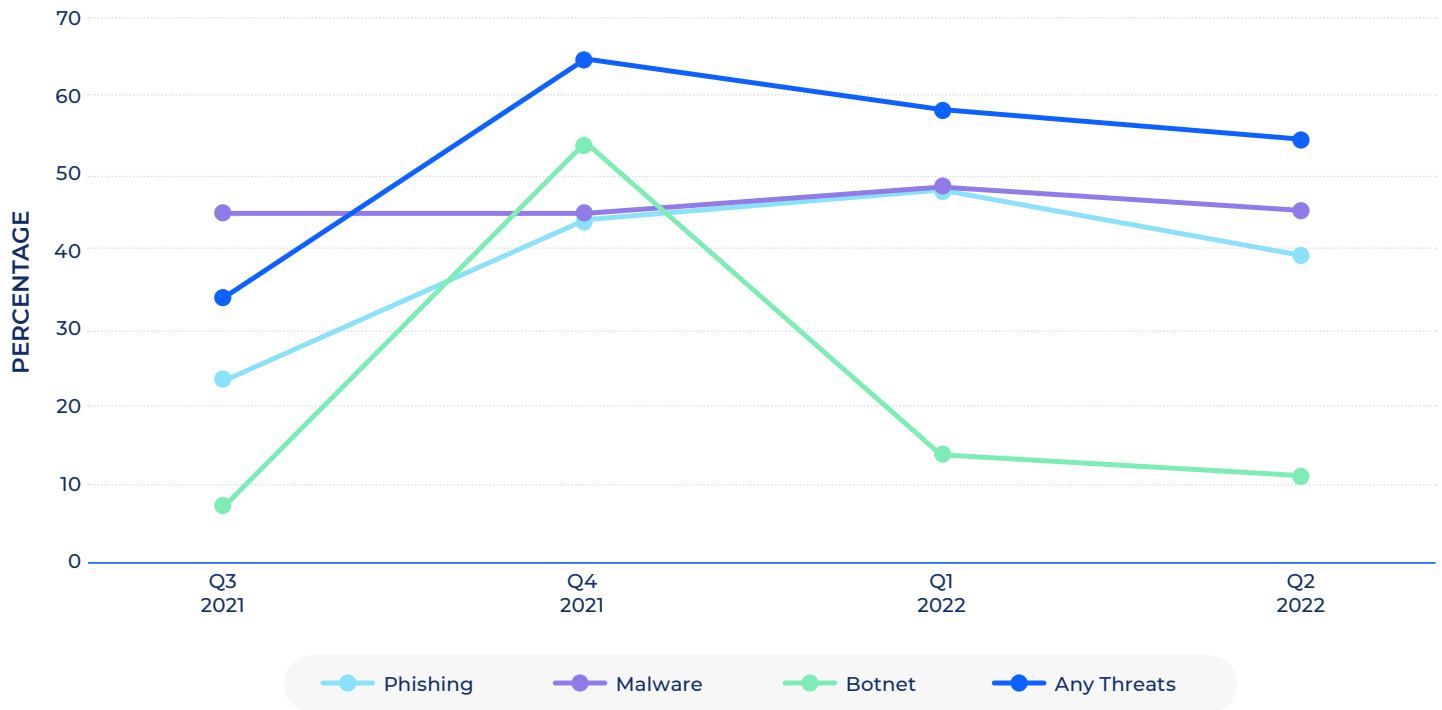
In Q2 2022, SecurityEdge™ threat lists added an average of 13,000 phishing entries, 86,000 malware entries and 75,000 bot entries each day. Customers who enroll in SecurityEdge™ need only the Comcast Business Internet and gateway supplied by Comcast Business. The service is easily managed through the customer portal.



Helping to Protect SMBs

The following charts represent 12 months of data collected by SecurityEdge™ (July 2021 to June 2022) on the types of threats against our customers, and attacks blocked by our security solution.

% OF BUSINESSES WITH BLOCKED ATTACKS (BY QUARTER)




Source: Comcast Business SecurityEdge™/Akamai Research

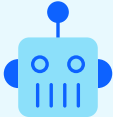
% OF BUSINESSES WITH BLOCKED ATTACKS (YEARLY AVERAGE)



38%
Phishing



45%
Malware



22%
Botnet



52%
Any Threats

Source: Comcast Business SecurityEdge™/Akamai Research

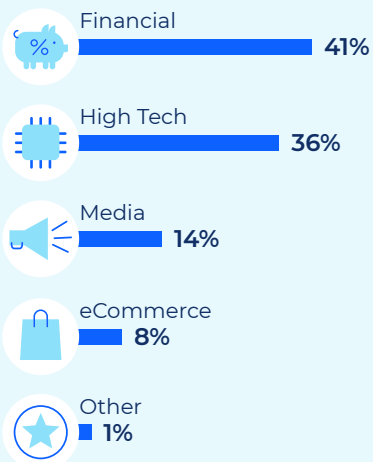


Helping to Protect SMBs: Phishing Activity

Websites owned by financial services and high-tech organizations are prime targets for phishing attacks.

Demand is high on the Dark Web for credentials stolen from those sectors. Akamai research shows in the most recent quarter (Q2 2022) financial and high-tech brands were the most targeted, at 41% and 36%, respectively.

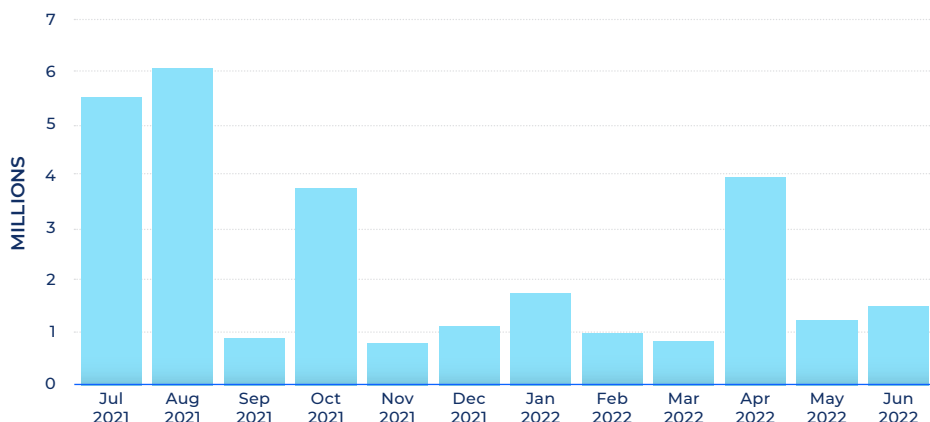
MOST TARGETED INDUSTRIES BREAKDOWN



Source: Akamai Research

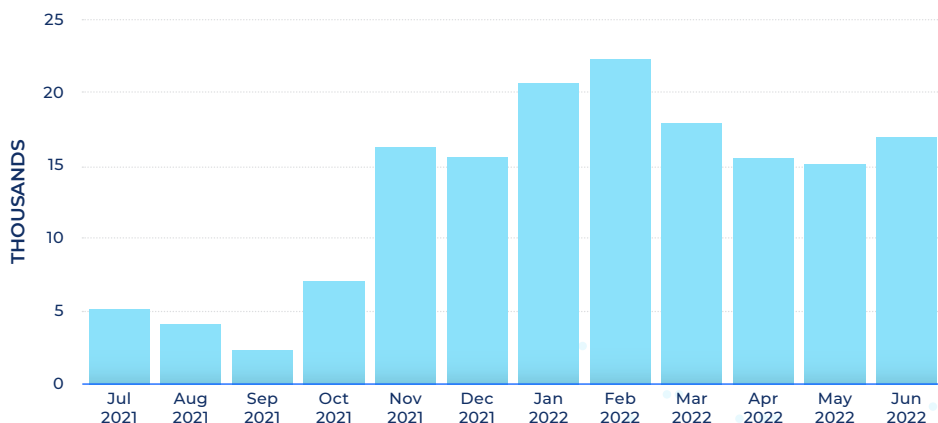
A wide range of phishing campaigns enabling ransomware, offering fake prizes, demanding unnecessary payments, stealing credentials and more were identified and blocked.

PHISHING ATTACKS BLOCKED BY SECURITYEDGE™ (DAILY AVERAGE BY MONTH)



Source: Comcast Business SecurityEdge™/Akamai Research

BUSINESSES WITH PHISHING ACTIVITY BLOCKED BY SECURITYEDGE™ (DAILY AVERAGE BY MONTH)



Source: Comcast Business SecurityEdge™/Akamai Research



Helping to Protect SMBs: Phishers' Tricks

Attackers who use phishing are skilled in targeting human attributes such as trust, fear and distraction to trick users into clicking links leading to compromised websites designed to appear legitimate. Check out some examples of the tricks:

Create typos that evade a quick glance.

✗ login.moffice356.com

✓ login.moffice365.com

Shift the familiar name to the left.

✗ apple.com.brlb.ru

✓ apple.com

Use a different top-level domain.

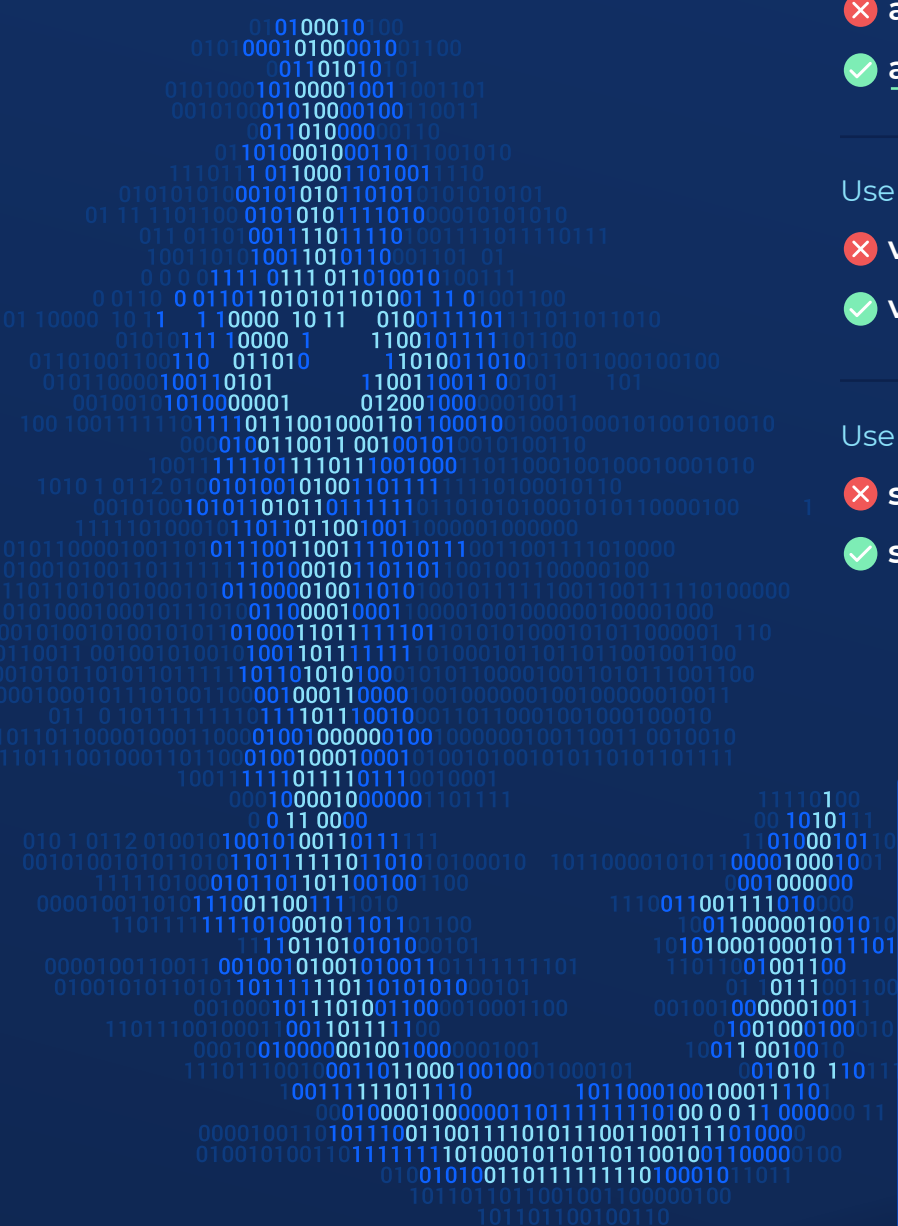
✗ verifyppal.xyz

✓ verifypaypal.com

Use non-latin lookalike character sets.

✗ singaporeair.com

✓ singaporeair.com



MOBILE CONCERNS

Mobile devices can be especially vulnerable to phishing because:

- Small screens have less room for threat alerts
- Users miss threat cues when scrolling
- UIs emphasize graphics over text, providing fewer signals for a threat
- Shortened or hidden URLs limit information to assess their legitimacy
- Users on the go tend to focus on completing tasks, not being cautious



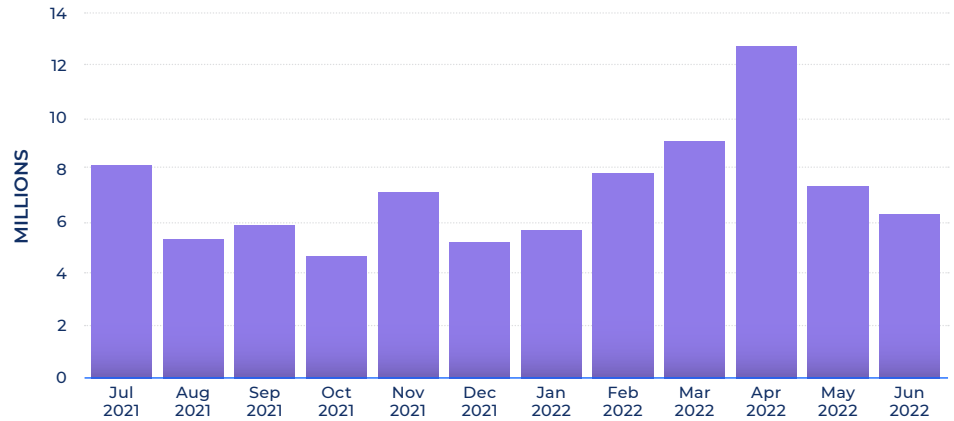
Helping to Protect SMBs: Malware Activity

Malware is another threat unsuspecting users face. Hackers have a myriad of tricks to load malicious software from websites.

Over the past year, SecurityEdge™ blocked websites used by hackers to host malware supporting cryptocurrency scams to gain access to user funds. The venues where the scammers collaborate were also uncovered and blocked.

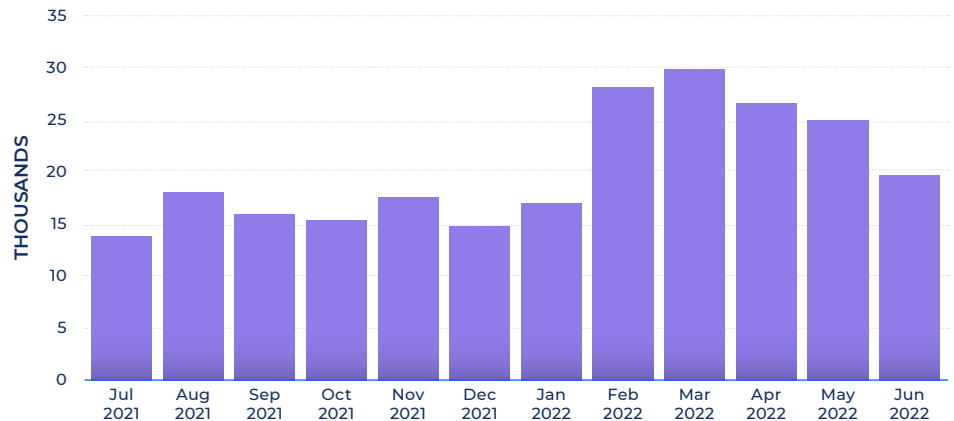
Malware activity was highly variable and diverse. Peak actions observed and blocked included stealing and secretly mining cryptocurrency, gathering private information from computers, and enabling malware to continue to spread.

MALWARE BLOCKED BY SECURITYEDGE™ (DAILY AVERAGE BY MONTH)



Source: Comcast Business SecurityEdge™/Akamai Research

BUSINESSES WITH MALWARE ACTIVITY BLOCKED BY SECURITYEDGE™ (DAILY AVERAGE BY MONTH)



Source: Comcast Business SecurityEdge™/Akamai Research



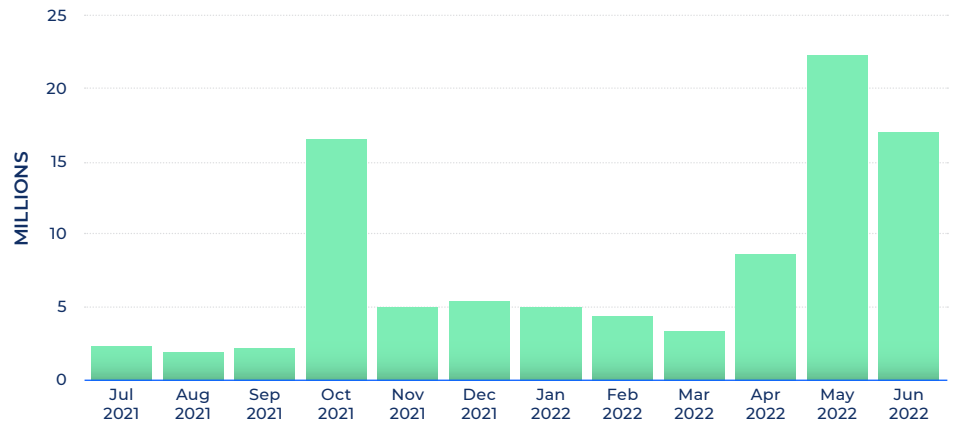
Helping to Protect SMBs: Bot Activity

A common type of cyberattack we've seen throughout the year involves bots enabling specialized DDoS attacks to target critical computing resources and websites to shut them down or disrupt service.

Akamai researchers also found and blocked large-scale botnets that use new features to hide malicious activities such as phishing, web proxying, and malware delivery. Also identified were illegal-market websites selling stolen credentials, hacked credit card numbers with Card Verification Values (CVVs), and venues professional hackers use to collaborate.

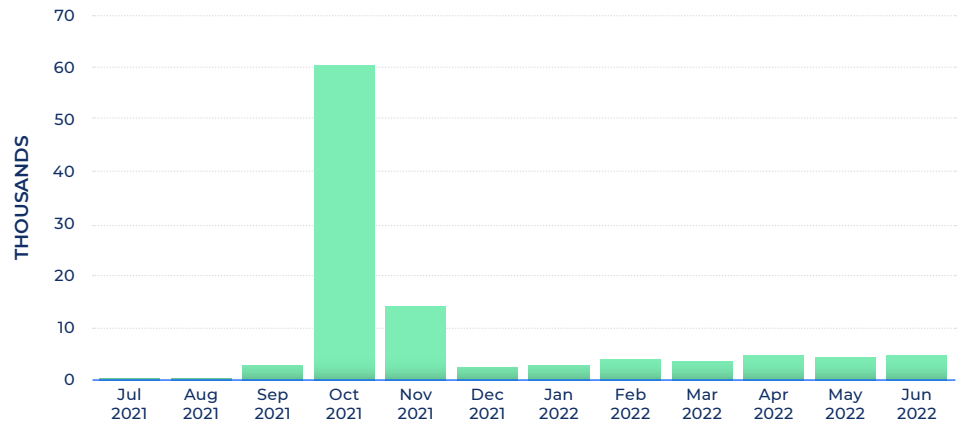
Bots were busy over the year. Very large bursts of activity enabled denial of service attacks and supported other parts of the malware ecosystem.

BOTS BLOCKED BY SECURITYEDGE™ (DAILY AVERAGE BY MONTH)



Source: Comcast Business SecurityEdge™/Akamai Research

BUSINESSES WITH BOTS ACTIVITY BLOCKED BY SECURITYEDGE™ (DAILY AVERAGE BY MONTH)



Source: Comcast Business SecurityEdge™/Akamai Research

Conclusion

Robust cybersecurity is essential for businesses of all sizes.

SMBs are targets of cyberattacks because they have valuable assets threat actors know how to monetize, and often lack sufficient defenses and resources to address the risks they face. They need an affordable security solution to help protect against cyberthreats.

Comcast Business helps address this need with Business Internet service coupled with Comcast Business SecurityEdge™ and leased router. Over the past year SecurityEdge™ blocked tens of millions of threats and helped protect tens of thousands of SMBs.



“ My small business doesn't have the luxury of a dedicated IT department. With Comcast Business SecurityEdge™, I can rely on Comcast Business to help protect my network and connected devices. In turn, I can spend time growing my business and not worrying about online threats. ”

- James Rice, CEO at Fiction Tribe, Portland, OR

COMCAST
BUSINESS