2023 Comcast Business

Small Business Cybersecurity Report

COMCAST
BUSINESS

As small businesses expand their digital footprint and their support of hybrid work models, they are at an increased risk for cyberattacks. Staying on top of the constantly changing threat landscape can be challenging without insights necessary to drive business decisions. Our second annual Comcast Business Small Business Cybersecurity Report provides an inside look at the current cyber threat landscape, through anonymized threat data gathered from fixed and mobile devices using our SecurityEdge™ service from July 2022 to June 2023. It also includes security insights from our partner Akamai and explains how our service helps deter malicious activity.

Executive Summary

With more devices than ever connected to the Internet, cybercrime has become a booming business. Criminals anywhere in the world can launch exploits at any time, against any targets they want, thanks to the ready availability of online tools that make it simple to modify their exploits and avoid detection.

Moreover, cybercrime is no longer relegated to individual rogue bad actors in dimly lit basement rooms – it is now being perpetrated by online organized criminal groups[1] and nation-states, who consider it a relatively low risk, high ROI endeavor.

While cyberattacks on large organizations like banks, health systems and government agencies tend to make headlines, small businesses are equally vulnerable. In their Cyber Readiness Report 2022[2] insurance provider Hiscox found that 48% of companies reported a cyberattack, and smaller US firms (less than 1,000 employees) reported a 7% increase in cyber attacks in the past year.

48% of companies reported a cyberattack in 2022.

7% ↑ in cyberattacks against small businesses in past year.

Why are businesses such an attractive target for cyber criminals? One reason is the proliferation of remote work. With more devices – including mobile and off-net devices – connected to the Internet from outside the office or primary place of business, attackers have more points of entry, creating new, complex layers in the cybersecurity mix.[3]

Mobile devices in particular tend to be overlooked from a security perspective due to the perception that cellular networks are secure. Cellular networks themselves are secure, but when phones access the Internet they're exposed to threats, especially phishing.

> "For smaller groups or individual criminals, these services can be hired on the cyber criminal 'online marketplace' using a plug and-play approach to crime."
>
> — **National Cyber Security Center Cyber crime:** understanding the online business model

[1] https://www.ncsc.gov.uk/files/Cyber%20crime%20-%20understabnding%20the%20online%20business%20model.pdf
[2] https://www.hiscox.com/documents/Hiscox-Cyber-Readiness-Report-2022.pdf
[3] https://lp.sosafe.de/hubfs/SoSafe%20-%20Human%20Risk%20Review%202022%20-%20EN-1.1.pdf

The Costs of a Data Breach

The Identity Theft Resource Center's 2022 Business Impact Report uncovers the financial impact of breaches on small businesses. Although revenue losses were slightly less than in their 2021 report, they were still costly and disruptive for these companies.

In addition to financial losses, more than 30% of businesses lost customer trust or had difficulty responding to customer concerns. Other challenges small businesses may face when hit with a cyberattack include lost productivity associated with efforts to restore compromised systems and devices. Notifying customers, vendors, investors/bankers and other partners may lead to lasting reputational damage with unknown costs. Finally, discovering and repairing a breach can be stressful and costly.

According to Hiscox, businesses are getting the message about the importance of cybersecurity. The firms they surveyed indicated an improved awareness of cyber threat exposure as the dominant risk to business in the US — ahead of the pandemic, economic downturn, skills shortages and other issues.

It is more critical now than ever that businesses implement protections and processes to help ensure a cyberattack doesn't cause disruption and all the associated costs that come with it.

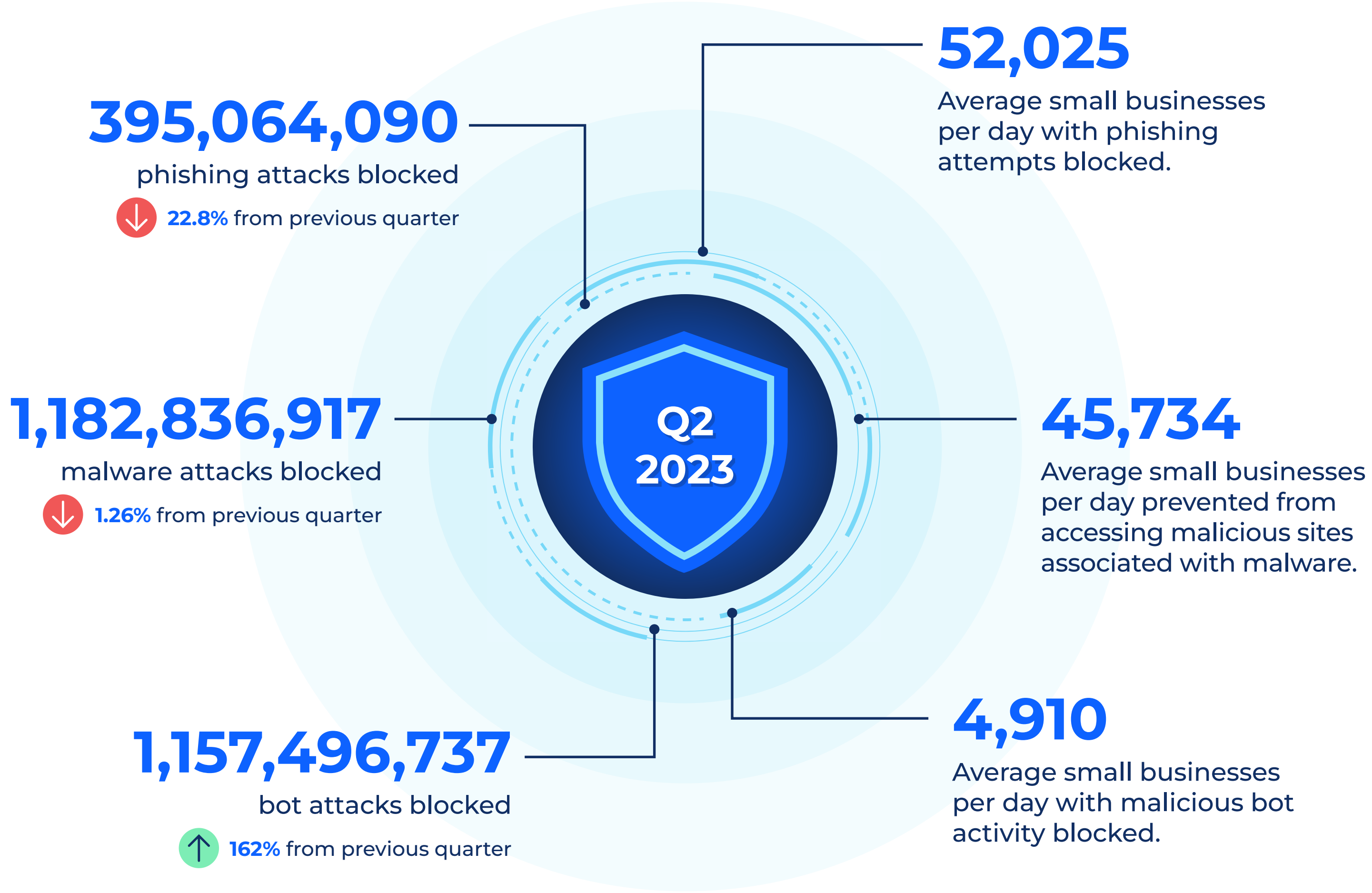
45%+ of small businesses reported a loss in revenue due to cybercrimes.

11% ↑ in revenue loss of less than $250K

6% ↓ in revenue loss between $250K-$500K

Threat Data Insights

Over the 12 months from July 2022 to June 2023, Comcast Business tracked cyber threats through its SecurityEdge™ cybersecurity service and found that small businesses were under near-constant threat from cyber attacks. **In the second quarter of 2023 alone:**



395,064,090
phishing attacks blocked
↓ **22.8%** from previous quarter

52,025
Average small businesses per day with phishing attempts blocked.

1,182,836,917
malware attacks blocked
↓ **1.26%** from previous quarter

45,734
Average small businesses per day prevented from accessing malicious sites associated with malware.

1,157,496,737
bot attacks blocked
↑ **162%** from previous quarter

4,910
Average small businesses per day with malicious bot activity blocked.

Source: Comcast Business SecurityEdge™/Akamai Research

1 out of **10** Mobile Devices

Attempted to reach out to domains associated with malware, phishing or malicious bots.

Inside the Attacks

Akamai collects data on Internet traffic across the full spectrum of industries and geographies. Comcast Business, through its SecurityEdge™ service, gathers insights on cyber threats against small businesses.

Here, we present an inside look at the cybersecurity issues companies faced between July 2022 and June 2023.

Akamai's visibility into daily fixed and mobile Internet traffic across industries and geographies from Q3 2022 to Q2 2023 showed daily malware activity roughly doubled year over year, with peaks in both holiday seasons. Although phishing activity trended downward over the course of both years, based on a daily average, it increased about 325%. Bot activity grew steadily over both years, with very large bursts of activity in May 2022 and May 2023.

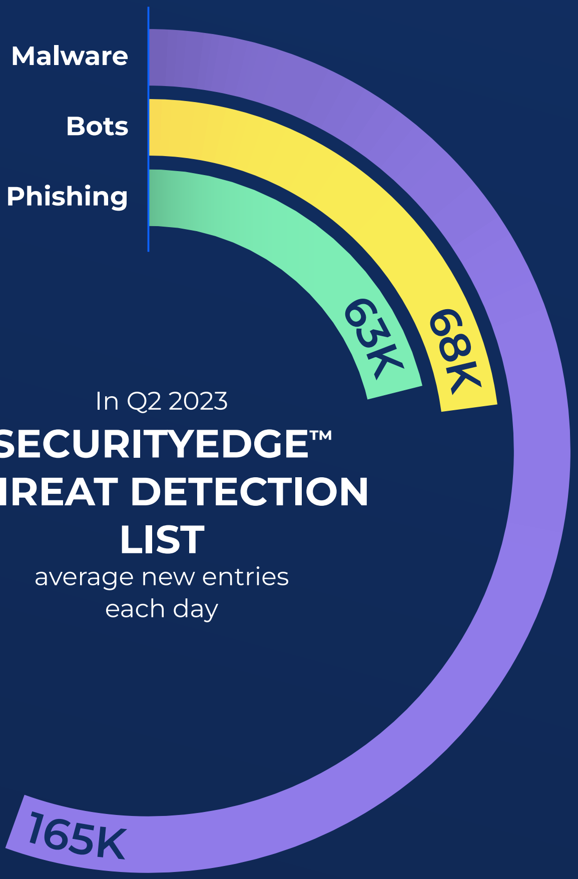
Akamai analysis of DNS traffic from mobile devices from Q2 2022 to Q1 2023 showed that nearly 1 in 10 devices, on average, attempted to reach out to domains associated with either malware, phishing, or malicious bot domains (also called command and control or C2).

Over twelve months (Q3 2022 to Q2 2023) Comcast Business tracked cyber threats through its SecurityEdge cybersecurity service and found that small businesses were under regular threat from cyber attacks.

In Q2 2023 alone for example, SecurityEdge™ cybersolution lists were updated by an average of nearly 68,000 phishing entries, over 165,000 malware entries and nearly 63,000 bot entries each day (rounded to the nearest thousand).

Comcast Business SecurityEdge™

A simple, affordable and easy-to-manage cloud-based cybersecurity solution, SecurityEdge actively checks all outbound Internet traffic, including off-net devices via Extended Coverage, with updates based on the latest cyberthreats every 5 minutes.



In Q2 2023

SECURITYEDGE™ THREAT DETECTION LIST

average new entries each day

Blocking Attackers

In separate, single-day incidents,

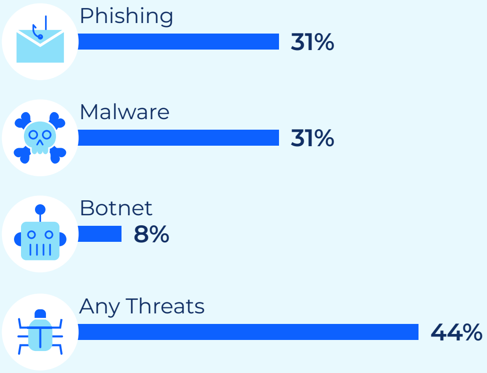
SecurityEdge successfully:

- Blocked 28 million phishing attempts and helped protect 81,793 small businesses against phishing.
- Blocked more than 60 million accesses to websites associated with malware, preventing users at 69,485 small businesses from accessing malicious websites.
- Blocked more than 37 million instances of malicious bot activity for 38,946 small businesses.

Looking more broadly, twelve months of SecurityEdge data from Q3 2022 to Q2 2023 shows the percentage of businesses faced with threats each month.

SECURITYEDGE SUBSCRIBERS EXPOSED TO

(YEARLY AVERAGE OF MONTHLY DATA)



28 Million
Phishing attempts blocked

81,793
Small businesses protected from phishing attempts

60 Million
Malware attempts blocked

69,485
Small businesses protected from malware attempts

37 Million
Malicious bot attempts blocked

38,946
Small businesses protected from bot attempts

Phishing, Malware & Bots:
The Terrible Three

Criminals use a variety of methods to target the devices that workers and businesses depend on. These are the three most common.

PHISHING

Web links in emails, texts, or other places designed to encourage clicks that take people to malicious web sites where valuable personal information can be harvested and monetized.

MALWARE

Malicious software designed to locate and steal valuable data, encrypt data and demand payment, damage or disrupt devices, or gain unauthorized access to a network.

MALICIOUS BOTS

Software secretly installed on computers and remotely controlled. Networks of bots find and upload valuable information, launch Denial of Service attacks, provide access to machines and more.

Phishing Activity Blocked

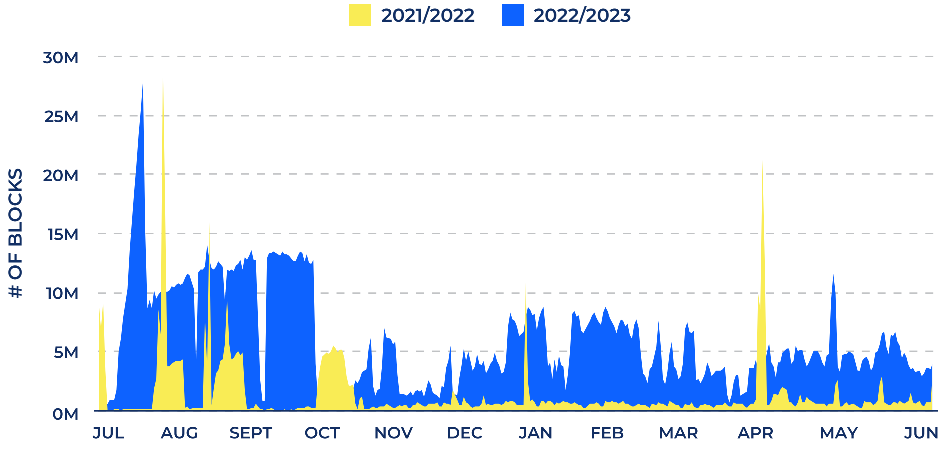
Phishing attacks trick people into clicking on malicious website links, allowing cyberthieves to harvest valuable personal information.

Attackers seek to make money by selling stolen credentials in darknet markets or logging into sites directly to access financial accounts and monetize stolen data.

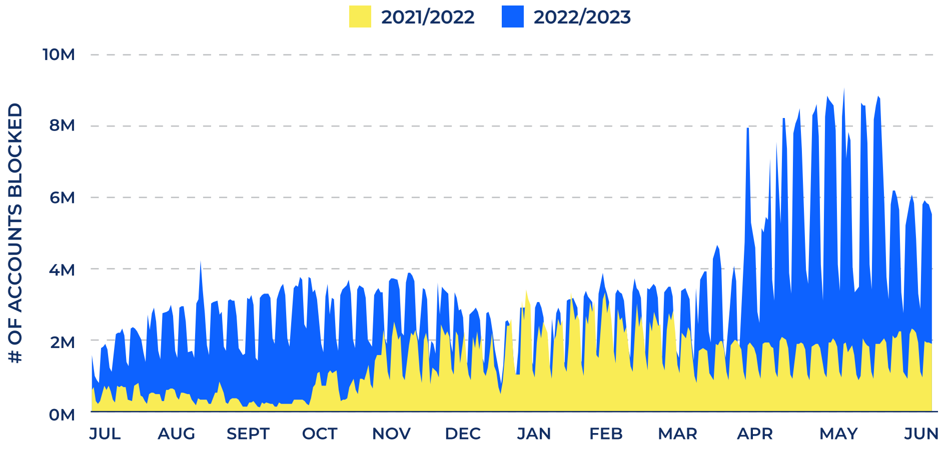
> "Phishing attacks are a persistent cybersecurity threat against organizations. Furthermore, phishing attacks no longer target only desktops or laptops. Mobile devices are now a prime target as well that require careful attention."
>
> — **National Cybersecurity Center of Excellence**, National Institute of Standards and Technology[4]

Twelve months of SecurityEdge data from Q3 2022 to Q2 2023 shows the number of phishing attempts blocked and the number of businesses with devices that attempted to reach malevolent web sites associated with phishing.

PHISHING ATTACKS BLOCKED BY SECURITYEDGE™ (DAILY)



BUSINESSES WITH PHISHING ACTIVITY BLOCKED BY SECURITYEDGE™ (DAILY)



DAILY AVERAGE PHISHING ACTIVITY

↑ **325%**
Increase in phishing activity overall YoY

↑ **150%**
Increase in businesses protected overall YoY

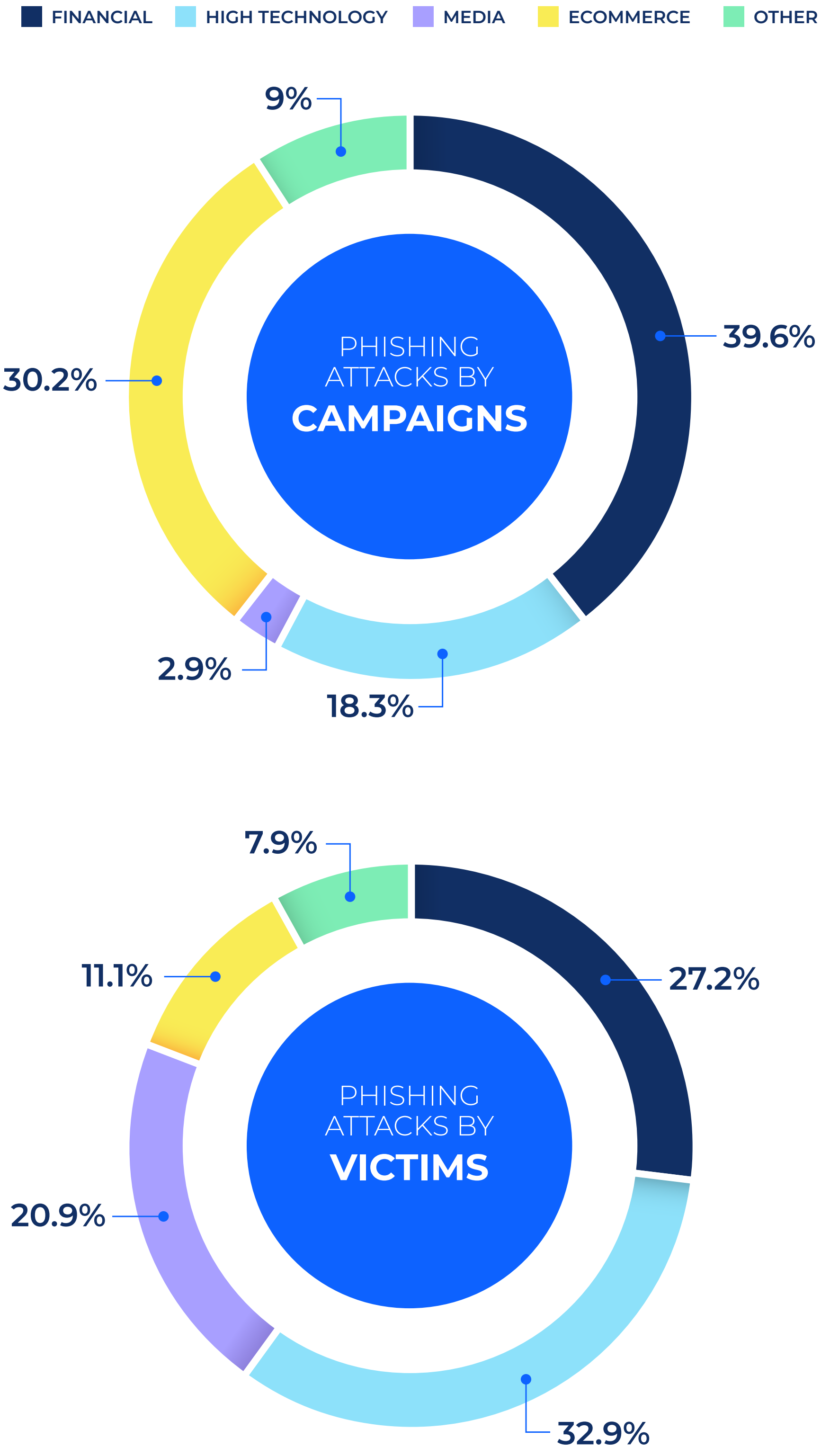
[4] https://www.nccoe.nist.gov/sites/default/files/2022-06/Phishing-Short-Form.pdf

Targeted Industry Breakdown

Akamai data showed financial services, technology, media, and ecommerce companies are the most common targets for phishing.

Akamai analysis in Q1 2023 found financial brands had the highest number of phishing attack campaigns (39.6%), but only 27.2% of victims. High technology brands and services had the opposite trend: 18.3% of the phishing campaigns and 32.9% of the victims. Although the data suggests attacks against financial services were relatively less effective, they may be more lucrative, given the direct connection to money from financial accounts.

MOST TARGETED INDUSTRIES BREAKDOWN



4. https://www.nccoe.nist.gov/sites/default/files/2022-06/Phishing-Short-Form.pdf

Stay Off the Hook: Ways To Avoid Phishing Attacks

Phishing remains a persistent problem and can lead to many types of cyber attacks.

Businesses may go to great lengths to protect their network and data, but often, people are weak links in the cybersecurity chain. Threat actors abuse visible brand names and have become skilled at changing their strategies to manipulate our emotions and actions. Here are some common methods they use and ways to stop them in their tracks.

Look carefully for typos in domain names

✗ Remote.casinc.biz_casinc

✓ Remote.casino.biz_casino

Watch out for transposed letters or numbers

✗ login.moffice356.com

✓ login.moffice365.com

Check top-level domains (TLD)

✗ apple.bid

✓ apple.com

Check website name

✗ apple.com.brlb.ru

✓ apple.com

Check for letters and numbers that look alike

✗ 0utlookwebaccess

✓ Outlookwebaccess

If something feels off, paste it into a search bar to see what happens

✗ googleplusforus.com — is not a Google web property

ADDITIONAL TIPS!

Be extra cautious when you’re using mobile devices. Small screens make it harder to see little details that reveal scams.

When you’re on the go take an extra moment before you click on links that are unfamiliar, **phishers love distracted users!**

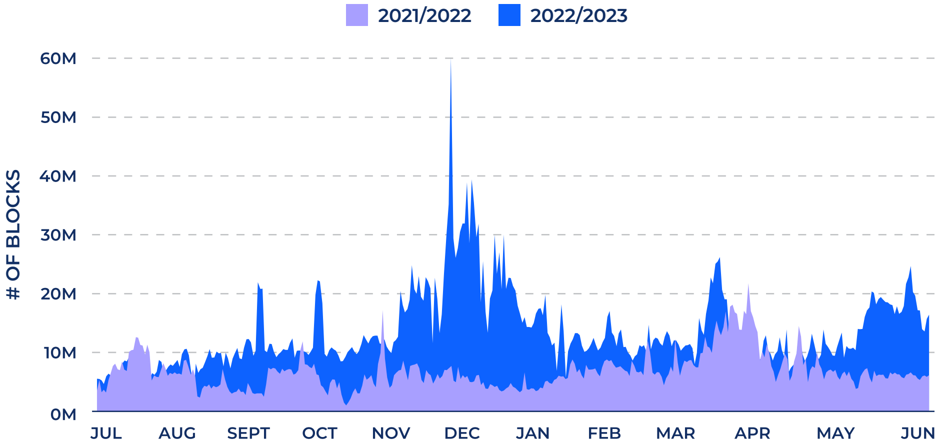
Malware Activity Blocked

Malware is malicious software designed to locate and steal valuable data, encrypt data and demand payment, damage or disrupt devices, or gain unauthorized access to a network.

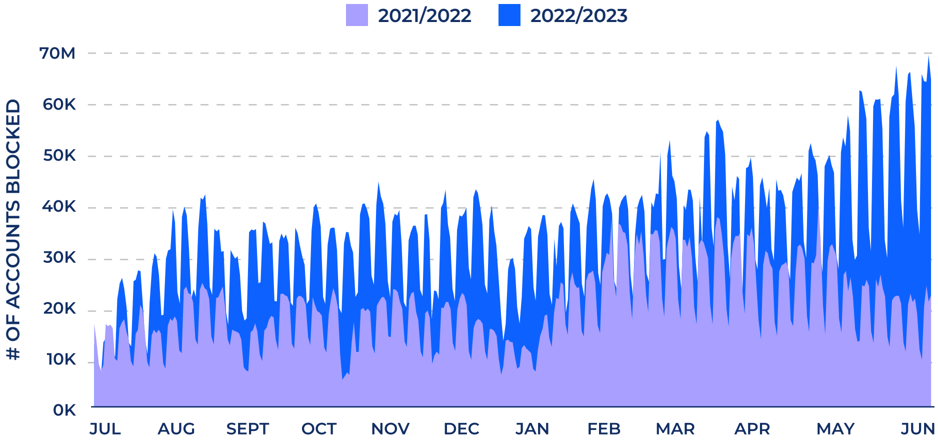
Malware developers are using increasingly sophisticated methods to design and distribute their malware attacks, often by using phishing and targeting users' mobile devices to gain access.

Twelve months of SecurityEdge data from Q3 2022 to Q2 2023 shows the prevalence of malware activity targeting businesses. These trends indicate more consistent activity on the part of threat actors as they spread their exploits more effectively, resulting in more activity over time. Throughout most of the year there were large spikes of activity associated with malware that contains the name of prominent security researcher Brian Krebs in the domain name it uses.

MALWARE BLOCKED BY SECURITYEDGE™ (DAILY)



BUSINESSES WITH MALWARE ACTIVITY BLOCKED BY SECURITYEDGE™ (DAILY)



DAILY AVERAGE MALWARE ACTIVITY

↑ **97%**
Roughly doubled overall YoY

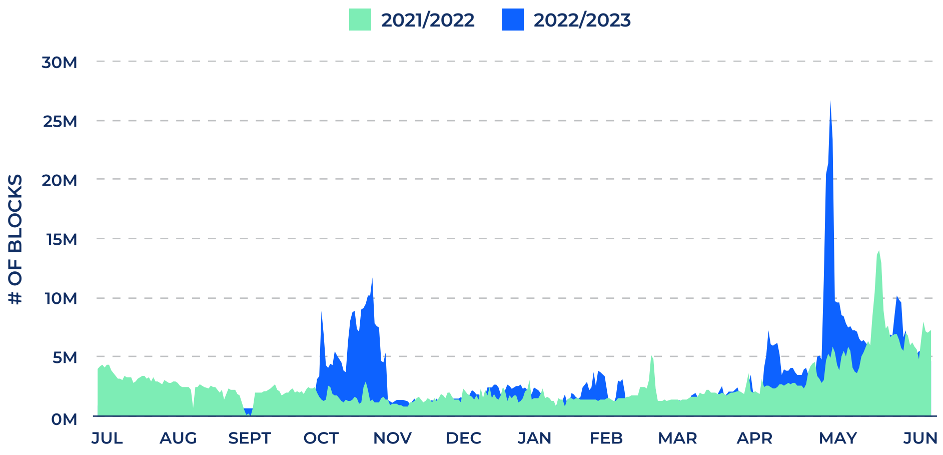
↑ **75%**
Increase in businesses protected overall YoY

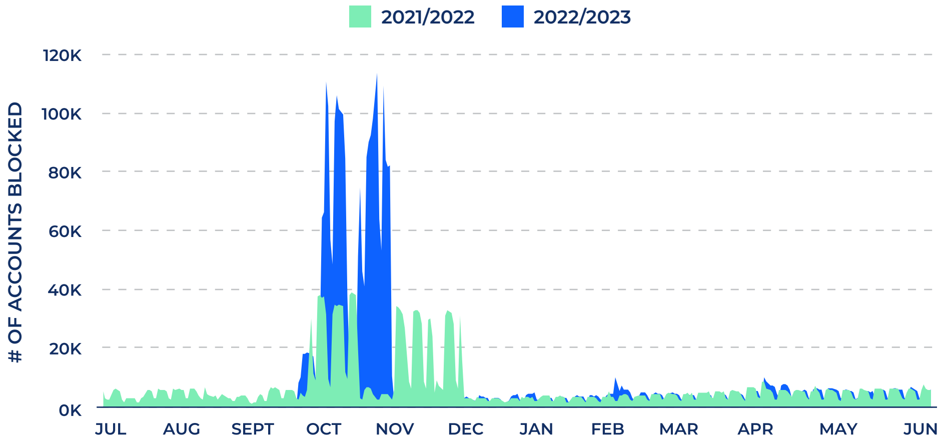
Malicious Botnet Activity Blocked

Bots are software programs secretly installed on computers and remotely controlled by a botmaster using what's known as "command and control" or "C2", to issue directives to infected digital devices.

Bots are remotely controlled to do many things, like steal valuable information, or look for other machines on a network to infect. Some bots are completely programmable with sophisticated controls so their functions can be changed over time. There have been some visible bot campaigns targeting mobile devices.

Twelve months of SecurityEdge data from Q3 2022 to Q2 2023 shows the prevalence of botnet activity and businesses protected from it. It is interesting to note that although the spike in overall bot activity in October and November of 2022 was small, there was a significant increase in the number of businesses experiencing such activity, leading to the conclusion that criminal organizations managing bots may have temporarily found a more effective way to distribute their exploits among a larger group of targets.


BOTS BLOCKED BY SECURITYEDGE™ (DAILY)


BUSINESSES WITH BOTS ACTIVITY BLOCKED BY SECURITYEDGE™ (DAILY)

DAILY AVERAGE BOT ACTIVITY

Bot activity grew steadily over both years, with very large bursts of activity in May of 2022 and 2023. The number of businesses protected trended down during each year.

Looking Forward: Businesses of All Sizes Need Robust Cyber Security

Threat actors and criminal groups constantly innovate their tools and strategies to ensure they can continue to expand their efforts, evade detection, and monetize their exploits.

They work diligently and strategically to understand how security defenses operate and build new ways to evade them through resilient and redundant evasion tactics that delay detection and takedown as long as possible. There is no reason to believe attackers will slow these efforts.[5]

As businesses continue to adopt remote and hybrid work policies that require the use of off-net and mobile devices to access applications and data, they will become an increasingly attractive target for cyber criminals. Small businesses are not immune from losses that can impact their operations, profit and reputation.

[5] https://www.akamai.com/blog/security-research/never-ending-sophisticated-phishing-scam-campaign

Comcast Business SecurityEdge™

Comcast Business SecurityEdge™ helps protect Internet 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.

New features extend to help protect workers when they use PCs, mobile phones, or tablets away from the office. The service is easily managed through an Internet customer portal and no additional equipment is required other than a leased router. Over the past year, SecurityEdge™ blocked tens of millions of threats and helped to protect tens of thousands of small businesses, both on their premises and remotely.

> “I look forward to viewing the SecurityEdge Activity Summary Report. It tells me about our network threats including phishing, malware, and botnets. We are comforted that it helps protect our employees’ and customers’ devices."
>
> **— James Rice**
> CEO, Friction Tribe

Protection for remote devices

Protect remote employee devices like PCs, mobile phones and tablets when used away from the office.

Easy set up, no extra equipment

All you need is Comcast Business Internet (or Ethernet Dedicated Internet, where available) and Comcast Business leased or managed Router. All design, installation, change management and equipment maintenance is included.

Visibility anytime and anywhere

See what is happening on your network by monitoring blocked threat activity via a personalized dashboard and email reporting.

Security regularly updates and looks for new threats

Offering updates of global threat intelligence every 5 minutes.

Content filtering and blocking

Businesses can set up personalized filters to block use of unwanted websites by employees and customers.

COMCAST
BUSINESS