Adapting to the Unpredictable
Last year, the SOTI team pledged to evolve, but we had no idea that the evolution before us would require such dramatic changes to how we both live and work. In truth, 2020 was a roller coaster with dramatic ups and downs, encompassing stress, fear, and uncertainty. Even as 2021 unfolds, COVID-19 is still impacting our day-to-day lives at work and at home.

For this first edition of SOTI Research, we’re going to look back at 2020 and examine some of the technological shifts that happened. Rather than simply talking about trends for the world as a whole, we’re also including a look into the attacks against our own systems to provide concrete examples.

Rather than simply talking about trends for the world as a whole, we’re also including a look into the attacks against our own systems to provide concrete examples.
The Internet Is Resilient

In April 2020, Martin McKeay (Editorial Director) published a blog article reporting that Akamai observed a 30% increase in internet traffic as pandemic lockdowns started to take hold. The big question for those shifting to work-from-home setups, distance learning, and complete lockdown/isolation was “Will the internet melt down?” – the short answer was, and still is, no.

Yet at the same time, the lockdowns and shift to remote functionality did have an impact on the internet. That 30% growth that McKeay’s blog article mentioned represented a year’s worth of growth in just a few short weeks. You can’t call that anything but significant.

As seen in Figure 1, the growth referenced persisted throughout 2020 as the general average – however, the entire year experienced traffic spikes. These spikes can be linked to various events, including summer vacations, holidays, sporting events, streaming media releases, and resurgence of COVID-19 mandates as spikes in the virus were recorded and addressed by local governments. On November 11, 2020, traffic hit a record-setting peak for a single day, when the monitors recorded 180 Tbps.

Fig. 1: Global traffic during 2020 as observed by Akamai; the rolling seven-day average is marked
Using the delta from the average set in February (pre-pandemic in the United States), we can see a few patterns that emerged in 2020, from the lockdown-related spikes toward the end of Q1 and in Q2, to the resurgent spikes in Q4 that were due to a mix of lockdowns and closures, as well as the holidays. There are other spikes, including a day in November that nearly doubled traffic levels, peaking at about 97% above the norm. That spike was then followed by dates in December peaking in the mid-70% range, climbing to the lower-80% range.

The traffic data also tells another story: a human one.

If you’re reading this, you experienced 2020 for yourself. Figure 1 tells the tale of remote learning, online gaming with friends in sessions that lasted long into the evening, video conferences and virtual hangouts, daily meetings, streaming movies and television shows at all hours, sporting events, and daily consumption of news and social media. The internet kept us working, learning, and connected. In some cases, it also caused us stress and anxiety – we’d be dishonest if we didn’t acknowledge that fact. But the main point is that the internet was there, it’s still here, and it will be here for a long time to come. The internet is resilient.

Defending Akamai During a Pandemic

Defending an enterprise against an attack is hard enough, but defending one where the majority of employees are remote is even harder. The transition from an office to home was a challenging process for businesses across the globe. Akamai was no exception. Security exists to enable, but people are not machines, and sudden changes to habits and workflows can cause difficulty. Thus, security needs to become somewhat fluid, adapting to the needs of the people it’s defending.
As we’ve discussed in past reports (such as State of the Internet / Security Vol. 5, Issue 5), Akamai uses its own products and services to defend ourselves. We were prepared for remote work, as the layered defenses in place could easily adapt to this business model. Our Zero Trust model enables remote workers to do their jobs from anywhere and protects them at the same time, but it’s taken years to architect this model to where it is today, and we’re still working on it.

One of the key layers of defense that Akamai uses is Enterprise Threat Protector, which uses Akamai’s research and data, augmented with third-party data, to identify malicious domains and block them at the DNS and HTTP level. It addresses several key elements used by criminals including exfiltration, command and control (C2), and phishing.

As the world went into lockdown in 2020, the criminals did too. This means they needed to shift their operations somewhat and start targeting workers who were at home rather than in the office. Criminals adopted new phishing lures (many of them focusing on COVID-19), targeting VPN credentials, videoconferencing applications, and personal information, which was used for financial and benefit fraud.
In 2020, Akamai faced 21,518,050 million malicious DNS queries out of an aggregate of 109 billion, or about 299 million DNS queries per day. Drilling down into the queries, which we see in Figure 2, the attacks were varied throughout the year, with peaks happening in Q2, Q3, and Q4.

There were 4,542,524 blocked requests to the C2 infrastructure of botnets in 2020, indicating a possible compromise. However, because the request was blocked, the system had no way to contact the C2 for instructions. For the C2 blocks that were recorded for this report, endpoints that attempted to connect to something known as hostile, either unintentionally or indirectly, such as potentially malicious content that is included within legitimate content as a person simply browses the web, were included in the count. As many in the IT and security space know, users will sometimes inadvertently open risky, or potentially malicious files, or they’ll inadvertently access malicious URLs through no fault of their own. When this happens, IT teams will speak to the system owner, alerting them to potential problems, if any exist. It’s also common to see IT teams offer additional awareness training if needed, or just reimage the system. In our case, because we used layered defenses, the blocks recorded in this dataset were mostly proactive because of third-party access. However, the exact nature of the block at the time it was made isn’t known.

Fig. 2: Logs from Enterprise Threat Protector show spikes in phishing and malware attacks in Q3 and Q4 2020
There were 10,155,209 blocked requests related to malware during this same period. This could be due to a malicious link being clicked in an email, document, or even on a website, but the exact cause of the block event remains unknown. Finally, there were 561,469 DNS exfiltration requests blocked, which was the least-observed method of attack during 2020.

Phishing, second only to malware, was the other top attack type observed in the Enterprise Threat Protector logs for 2020, with 6,258,597 blocked attempts. On the whole, Akamai is comparatively more targeted per industry comparisons when it comes to phishing, which is somewhat expected. Big companies are big targets, after all. Looking at the business units that were the most phished during the year, the results are a bit different than the last time we examined this data set.

In 2020, the top Akamai business units phished were our platform unit, finance division, global services, office of the CIO, and the web sales and marketing unit. But our support division (AkaTec) and media and carrier groups were also targets.

What this tells us is that criminals aren’t too picky when it comes to targets, but they will focus their efforts when the potential gain is large, such as compromising someone in the platform unit.

After a peak of C2 attacks in Q2, the majority of attacks happened in Q3 and Q4, with phishing and malware jumping out in totals, with 2,358,461 attacks in September and 1,863,693 attacks in October, respectively.

What this tells us is that criminals aren’t too picky when it comes to targets, but they will focus their efforts when the potential gain is large.
Conclusion

One of the lessons learned in 2020, as it pertains to remote work and distance learning, is that the usual way of protection will work to a degree, but security must adapt rapidly to changing situations. Just because a policy or program works great in a data center and office doesn’t mean it will work when everyone has to go home. The forced changes in 2020 were a blunt reminder of this fact.

Another takeaway is that just because your workers are remote, and the office is empty, doesn’t mean the criminals will take a break. Like your security program, criminals will adapt, shift focus, and do whatever they can to compromise credentials, financials, and everything in between. This is certainly clear when you look at the Enterprise Threat Protector spikes. The attacks were consistent all year long, but at certain times, criminals doubled – or even tripled – their efforts.

As this report is being written, the opening month of 2021 has come to a close, and February is well underway. We’re still remote, and we’re still seeing a consistent stream of attacks, not only at Akamai, but all across the globe. But we’re optimistic: We made it through last year and the challenges it posed, and we’ll make it through this too.

Stay safe!
Credits

SOTI: Research contributors

Editorial Staff

Martin McKeay
Editorial Director

Amanda Goedde
Senior Technical Writer, Managing Editor

Steve Ragan
Senior Technical Writer, Editor

Chelsea Tuttle
Senior Data Scientist

Marketing Staff

Georgina Morales Hampe
Project Management, Creative

Shivangi Sahu
Program Management, Marketing

More State of the Internet / Security

Read back issues and watch for upcoming releases of Akamai's acclaimed State of the Internet / Security reports. akamai.com/soti

More Akamai Threat Research

Stay updated with the latest threat intelligence analyses, security reports, and cybersecurity research. akamai.com/threatresearch

Access Data from This Report

View high-quality versions of the graphs and charts referenced in this report. These images are free to use and reference, provided Akamai is duly credited as a source and the Akamai logo is retained. akamai.com/sotidata

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world’s top brands trust Akamai, visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 03/21.