SNAPSHOT

THE MEDIA TRUST
We know digital security.

Digital Trends: May 2020

Changed environment driving more malware to end users

Key Learnings

- 25% month-over-month increase in active malware volume
- 31% malware increase detected in at-home environments since March
- Recommendations:
  - continuous client-side scanning of digital assets
  - real-time blocking

Fallout from the COVID-19 pandemic continues to reverberate throughout the broader digital ecosystem, propagating malware at unprecedented levels. The Media Trust's Digital Security & Operations team is managing significantly more malware volume than usual; the number of active incidents in a 24-hour period was an average 25% higher in May compared to typical daily volume. (Figure 1)

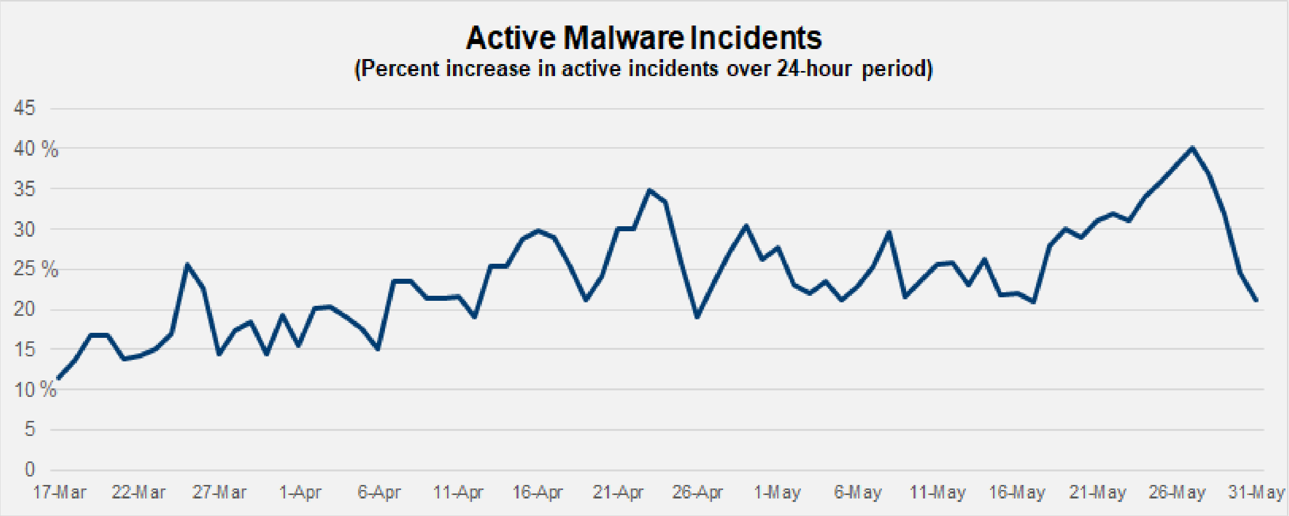

Figure 1: Active malware incidents managed in a 24-hour period

Malware behavior has changed, too. In addition to the anticipated rise in scams and fraudulent activities, malware incidents are now heaviest during the week, reversing a long-held pattern of spiking Friday through early Monday morning. While large-scale attacks still occur during the weekend, the mid-week volume has been atypically high since April.

The New Normal: Malware patterns target at-home users

This heightened malware volume is also reflected in “at-home” internet connections. Isolating U.S.-based at home providers (AT&T, Comcast, T-Mobile and Verizon-FIOS), malware detection rates grew 31% during the March to May period, continuing an upward trend that started in February and correlating with overall detection volume. During this period, malware grew by a factor of 1.5 on AT&T, Comcast and T-Mobile while AT&T experienced 3X growth. (Figure 2)

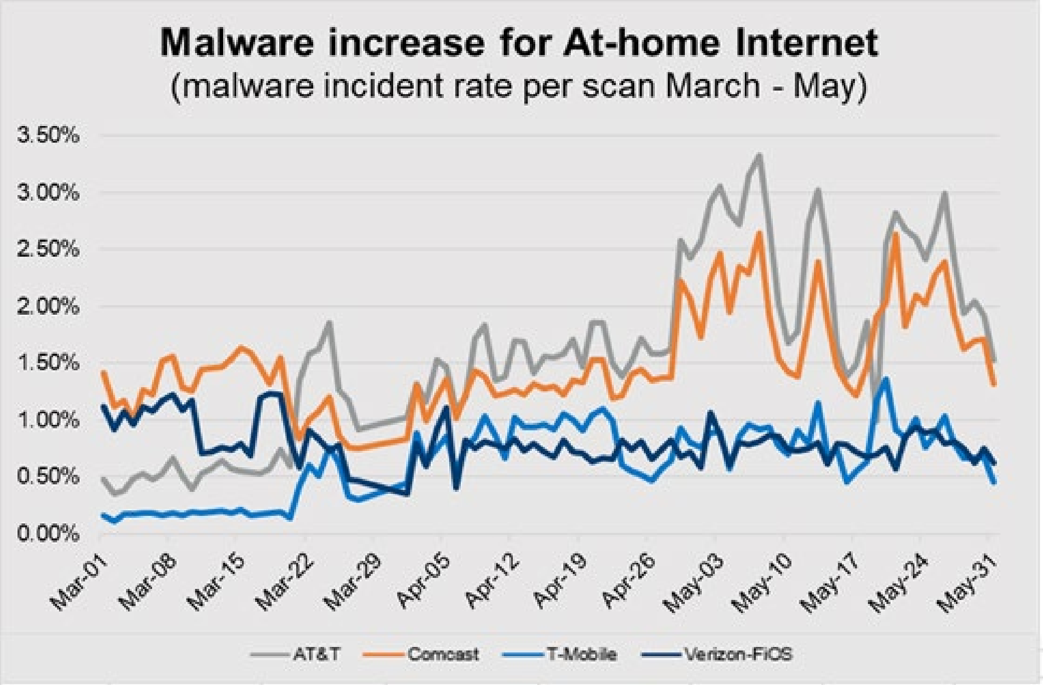

Figure 2: Malware affecting at-home internet end users

At the end of May, malware activity began to show signs of stabilization, beginning a downward trend that appears to flatten in early June. However, malware remains at an elevated level compared to historical rates during the past year, likely representing an alarming “new normal” in the digital advertising ecosystem. This inflated malware volume pressures existing security and operations teams and processes already stressed with managing the dynamic, sophisticated, and persistent nature of malvertising. Those without continuous scanning and blocking tools will likely experience more end user complaints associated with increased device infections and personal data exposure.

Malware exploits vulnerability of remote work behaviors

The increased internet traffic means consumers are being exposed to more malware when they read the news, purchase items, or search for entertainment. With more than 60% of employees now working from home, they are a malware target because many work off their home network and with multiple devices (sometimes obsolete) that lack the more stringent security controls found in a more traditional office setting.

This situation enables today’s malware proliferation. In addition to taking advantage of a lower barrier of entry due to depressed eCPMs, malvertisers benefit from a softer, more vulnerable end user target. Ad-supported websites and their partners need to consider how this changing malware environment affects end users and also how their own remote teams compound the situation. This includes adoption of trusted security tools to prevent malware from delivery in the first place.

Protect your end users. Protect your digital revenue.

In a customer-first and privacy-centric scenario, it’s imperative to protect the end user. Increased vigilance of digital partner activity is critical to thwarting attacks that negatively impact the user experience and its follow-on effect on revenue. This requires continuously scanning from a multitude of end user profiles to detect emerging and evolving malware techniques and feeding this up-to-date information into a real-time blocker. At a more strategic level, identifying and blocking partners that repeatedly violate your policies and/or traffic malicious content will drive a healthier, more user friendly digital advertising supply chain in the long term.