Adobe and Apple to Outpace Microsoft in 2017 Vulnerability Discoveries. So What Now?

Terms:
Jon Clay

Cybercriminals by and large don’t work to annual schedules. But as a new year rolls around again, there’s a valuable opportunity for organizations to take stock of their IT security posture and consider where the key threats lie over the coming 12 months. One major area highlighted in Trend Micro’s 2017 predictions report, The Next Tier[1], is in the number of software bugs discovered in non-Microsoft platforms.

It’s a trend we think will continue as Adobe and Apple outpace Microsoft in terms of newly discovered vulnerabilities. That’s going to make vulnerability shielding and better, multi-layered endpoint threat protection a must for organizations as we head into 2017.

Broadening their horizons

Microsoft was for years the only show in town for hackers. Much of that was due to its market dominance, despite the claims of rivals that their platforms were inherently more secure. But that’s changing now, and fast. Adobe outpaced Microsoft for the first time in 2016 in terms of new bug discoveries. And the year was Apple’s single biggest in terms of flaws as it too became a target.

When we wrote the report in November, the count for Microsoft was 76 new vulnerabilities – down from 160 in 2015, according to the TippingPoint Zero Day Initiative[2]. Compare that to 135 for Adobe, and 50 for Apple, more than double its 2015 haul.

Why is this happening? Well, Microsoft has certainly made great strides in developing more secure products thanks to the efforts of its Trustworthy Computing initiative. But we also have to look at market dynamics. Cybercriminals usually have one primary motive: making as much money as easily as possible. And this means targeting those platforms with the largest number of users. It ensures the bad guys generate the best possible RoI for any exploits they develop.

So, as we see Microsoft PC shipments decline while Mac and smartphone sales increase, this is going to have an impact on the number of new vulnerabilities discovered in these platforms. And as older software versions and models reach end-of-life, these too will come under greater scrutiny from the black hats. That’s why we believe we’ll see more exploits for flaws in the unsupported iPhone 4S this year.

Adobe software, meanwhile, has been a favorite of the hacking community for a while now – especially Flash. It too has a large installed user base, despite moves from many vendors to remove support. And its developers have been unable over the years to re-engineer the product in a way that radically improves security.

The fight back

What does this mean? A lot more of the same in 2017. Expect many more exploits targeted at Macs, unsupported iPhones and Adobe software. Many will be integrated into easy-to-use exploit kits, allowing even those with limited technical knowledge to launch attacks. And for those who think the demise of the notorious Angler EK[3] Spells good news for 2017, just remember previous iterations like BlackHole were replaced in time by yet another version.

There’s no silver bullet to solve these challenges. But you can go a long way by investing in products which offer vulnerability shielding. It’s the only way to reliably and proactively mitigate the risk of zero day and unpatched flaws.

There’s also clearly a need for more comprehensive endpoint protection, particularly against exploits targeting Apple and Adobe platforms. Trend Micro’s answer is XGen: a multi-layered cross-generational approach which combines proven and advanced protection techniques, such as application control, exploit prevention and behavioral analysis, with high fidelity machine learning.

It’s the only way to deal with a threat landscape evolving all the time. And an agile and persistent enemy.


Links: