Microsoft: From Zero to Hero in Internet Security

By Malcolm White, Vice-President, Portfolio Management and Portfolio Manager, Signature Global Asset Management
July 5, 2019

We recently attended the Gartner Security & Risk Management Summit held just outside Washington, D.C.

The Washington, D.C. area was an appropriate host for the conference given all of the internet security concerns raised by the current U.S. administration, including the security ban directed at China-based telecommunication equipment vendor Huawei Technologies Co. Ltd.

It is clear from the discussion at the conference that security hacking is no longer the domain of individuals or disgruntled groups. Organized crime has been involved for some time as hacking, especially for corporate espionage purposes, has proven to be a lucrative pursuit.

But the bigger headlines are the admissions from major nation states, including the U.S., that they, too, are not afraid to use hacking tools. Cyberwar is very real, as Iran and Russia will attest. So, no wonder cybersecurity is top of mind for any global organization.

The good news is cloud computing is helping companies to protect themselves by creating a real-time global security shield. Once a security threat is discovered on the internet, the cloud can be used to instantly update the security software for all companies that are connected.

The advocates of this strategy include next-generation security companies such as CrowdStrike Holdings, Inc. that recently launched its initial public offering.

Surprisingly, one of the leaders in this approach is Microsoft Corp. itself, the maker of computer software that was so easily hacked by cyberbullies and could not be patched immediately. Security breaches of Microsoft Windows 98 and 2000 operating systems forced the company to temporarily cease developing software until it could add security by default to its operating systems.[1]

[1] See the following: https://www.nytimes.com/2019/06/29/opinion/sunday/conficker-worm-ukraine.html
https://www.schneier.com/blog/archives/2009/10/ballmer_blames.html
https://searchsecurity.techtarget.com/Microsoft-Trustworthy-Computing-initative-causes-security-issues

Indeed, Microsoft recognized that security was becoming a problem as computers shifted from standalone desktops to fully connected internet devices running over untrusted public networks."[2]

Things are different at the new Microsoft. Sick of being the biggest target, the company has bulked up on security and is using its vast resources to fight back those cyberbullies.

Its secret weapon is what was once its greatest vulnerability: the Windows Operating System. New versions of Windows (e.g., Windows 10) have security embedded right into the operating system.

Combined with the cloud shield that we mentioned, Microsoft now has the ability to instantly update every machine, in real time, to protect it. The scale is staggering. Microsoft is analyzing 450 billion emails a month. It can do so because it has also been investing billions of dollars in its cloud computing infrastructure.

So, are we winning the war on cybersecurity? Or, perhaps the better question is whether this war is winnable at all.

If you read the headlines and talk to experts, cybersecurity still feels like the game of whack a mole; whack one security problem down and another appears.

But the new tools will help. This is one area where Artificial Intelligence is taking off both in terms of understanding the nature of the attacks and assisting with the automation of the appropriate response.

And this is not about technology replacing jobs. This is the opposite, in that there is a job deficit, with nearly four million unfilled positions in the cybersecurity field.

The technology is in fact making humans more efficient in keeping up with the volume of threats.

What is the biggest threat today, Stuxnet or some other crazy computer virus? Well, it still remains simple human behaviour that gets exploited by the bad guys. Using simplistic passwords and clicking on suspicious links in emails still remain the most common ways security is breached in an organization.

[2] https://www.cnet.com/news/gates-security-is-top-priority/

Despite all of the technological advances out there, common sense is still the best protection.

So when you get the next email from that mysterious stranger who tells you a fortune awaits in an overseas bank account if you just provide the following confidential details (I just received one just this past weekend), leave "too good to be true" where it belongs – safely put in your email recycle bin.

Sources: Signature Global Asset Management, New York Times and Bruce Schneier blog, as at June 30, 2019.

IMPORTANT DISCLAIMERS

The author and/or a member of their immediate family may hold specific holdings/securities discussed in this document. Any opinion or information provided are solely those of the author and does not constitute investment advice or an endorsement or recommendation of any entity or security discussed or provided by CI Investments Inc.

Commissions, trailing commissions, management fees and expenses all may be associated with mutual fund investments. Please read the prospectus before investing. Mutual funds are not guaranteed, their values change frequently and past performance may not be repeated.

The contents of this piece are intended for informational purposes only and not to be used or construed as an endorsement or recommendation of any entity or security discussed. The information should not be construed as investment, tax, legal or accounting advice, and should not be relied upon in that regard. Individuals should seek the advice of professionals, as appropriate, regarding any particular investment. Investors should consult their professional advisors prior to implementing any changes to their investment strategies. These investments may not be suitable to the circumstances of an investor. Some conditions apply.

Certain statements contained in this communication are based in whole or in part on information provided by third parties and CI Investments Inc. has taken reasonable steps to ensure their accuracy. Market conditions may change which may impact the information contained in this document.

Certain statements in this document are forward-looking. Forward-looking statements ("FLS") are statements that are predictive in nature, depend upon or refer to future events or conditions, or that include words such as "may," "will," "should," "could," "expect," "anticipate," "intend," "plan," "believe," or "estimate," or other similar expressions. Statements that look forward in time or include anything other than historical information are subject to risks and uncertainties, and actual results, actions or events could differ materially from those set forth in the FLS. FLS are not guarantees of future performance and are by their nature based on numerous assumptions. Although the FLS contained herein are based upon what CI Investments Inc. and the portfolio manager believe to be reasonable assumptions, neither CI Investments Inc. nor the portfolio manager can assure that actual results will be consistent with these FLS. The reader is cautioned to consider the FLS carefully and not to place undue reliance on

FLS. Unless required by applicable law, it is not undertaken, and specifically disclaimed that there is any intention or obligation to update or revise FLS, whether as a result of new information, future events or otherwise.

CI Investments and the CI Investments design are registered trademarks of CI Investments Inc. Signature Global Asset Management and Signature Funds are trademarks of CI Investments Inc. Signature Global Asset Management is a division of CI Investments Inc.

© CI Investments Inc. 2019. All rights reserved. “Trusted Partner in Wealth” is a trademark of CI Investments Inc.

Published July 5, 2019.

CI Investments® | Trusted Partner in Wealth™