Introducing our newest cybersecurity theme: Layer 8 - The Human Factor

Published December 5, 2022

WisdomTree
Contributor

Team8
Global venture group

In 2022 alone, there have been a growing number of high-profile cyber-attacks leveraging the ‘weakest link’ in every company’s security defences: the human factor. Preying on humans isn’t a new strategy for cybersecurity attackers; however, it is getting worse as we begin to see tools and tactics being applied in ways that are much more impactful.

What a teenage hacker did ten years ago as amusement, now has the potential to turn cities dark. Additionally, what an attacker could do by hacking someone in their personal space (smartphone, tablet, etc.) used to be very disconnected from their corporate world. But with everything that’s happened over the last two years with COVID-19 and remote work, the separation between personal space and corporate space has broken down. Thus, being attacked in your personal space has much more potential to leak over into your corporate space.

We’re seeing this play out due to three main drivers: broader availability of tools, new attack vectors, and emboldened attackers. For example:

- **Broader availability of tools** - tools that five years ago were only available to nation states are now available to criminal gangs, and tools that were only available to criminal gangs are now available to amateurs. As tools move down market, there is broader availability and a suite of new players. More dangerous tools and ‘government playbooks’ for the less skilled or disciplined creates a more reckless, dangerous environment.

- **New attack vectors** - because of digitisation and remote-work trends, there is an accelerated crossover of people's corporate lives with their personal devices and vice versa. Attackers are taking advantage of the fact that there is no longer a separation between those two personas and going after a person in their home where they don't have the defensive systems in place that they would in their corporate environment. One recent example of this was the Uber breach of September 2022 in which a teenage hacker, believed to be a member of the Lapsus$ hacking group, gained almost total administrative control over the company's computer systems, including software source code and internal messaging systems. The attacker gained access by bombarding the contractor's personal device with a multi-factor authentication (MFA) challenge, until he had no choice but to accept it, and even masquerading as a member of Uber's IT department to trick them into revealing their authentication credentials. The hacker then logged into the corporate VPN and roamed around the network, looking for targets[1].
- **Emboldened attackers** - there is a noticeable acceleration in the brazenness of today's threat actors, and their emboldened attempts at social engineering, such as by offering to pay the human beings employed by the company, its suppliers, and business partners of the target organisations for access to credentials and multifactor authentication (MFA) approval. Furthermore, attackers are quick to announce their feats on social media and even intrude in the internal incident response process of their targets, which puts more pressure on the victim while giving the attackers more leverage.

It's also worth mentioning that with the current macroeconomic environment and the potential for mass layoffs (for example, Twitter, which has cut half of its staff[2]; Meta, that's laid off 11,000 employees[3]; and Amazon, that's let go of 10,000 people in corporate and technology jobs[4]) the insider threat is growing, and organisations may find themselves at a higher risk for insider attacks. Moreover, another impact of COVID-19 is that many employees are being hired without ever meeting anyone from the company in person. This means that if someone has bad intent, it's a lot easier to infiltrate companies just by placing employees there. According to the Ponemon 2022 Cost of Insider Threats Global Report, insider threat incidents have risen 44% over the past two years, with costs per incident up more than a third to $15.38 million[5].

In response to the above threats and risks, we're seeing a robust set of solutions emerging that are focused on these problems, including but not limited to:

- Anti-phishing solutions
- Credential misuse prevention
- Social engineering and business email compromise solutions
- Breach attack simulation and other misconfiguration prevention tools
- Education, training, and awareness solutions for cybersecurity professionals, application developers, and everyday users
- Insider threat solutions including User Entity Behavior Analysis (UEBA) etc.

Because of the rising trend of attacks that leverage ‘human weakness’, converging at this point in time with the growing number of maturing dedicated solutions to combat them, we have decided to introduce a new cybersecurity theme to our list: Layer 8 - The Human Factor.

Layer 8 is a term used to refer to the ‘user layer’ on top of the 7-layer Open Systems Interconnection (OSI) model of computer networking[6]. What this means is that there are a number of security safeguards that don’t happen in the technology space at all - they are just the human control processes that surround, or in some cases operate in the absence of, the technology components of the system. At the end of the day, humans have an attack surface, they are part of the system, and therefore, security needs to pay attention to that attack surface and to mitigations that actually work in that environment.

Additionally, in the human layer, humans operate much slower and less efficiently than machines, which imposes a further limitation on their technological defenses. Making matters worse, these native limitations of humans create an attack surface that can only be mitigated by compensating controls, that is, you cannot patch a human. Every other layer besides the physical layer can be solved through patches.

According to Charles Blauner, Team8’s CISO in Residence and the former Global Head of Information Security at Citi, “As part of how security is done, we inherently have humans in the loop. No matter how much money a company invests in security controls, humans will always defeat them. Across every aspect of the space, we have to deal with how we take humans out of the equation. Humans make misconfigurations, humans get phished, humans have Excel spreadsheets with all of their usernames and passwords. A good red team always wins because the one thing that they can rely on is human weakness. Layer 8 is all about how we train humans, how we empower them, how we monitor them or, in certain instances, how we take them out of the loop.”

Although the human factor is an interesting, emerging theme that we are starting to officially track, it’s been a busy year in general for cybersecurity, be it in terms of geopolitics and the Russia-Ukraine war, deglobalisation, ransomware professionalisation, and cyber innovation. For better or worse, as it looks now, we expect 2023 to be no different. Please stay tuned for the full updated list of 2023 themes driving the future of cybersecurity growth, which will be announced in the beginning of 2023.

Team8 Disclosure

This Layer 8 - The Human Factor Article represents the opinions of Team8 Labs Inc. (“Team8”) and is for informational purposes only. You should not treat any opinion expressed by Team8 as a specific inducement to make an investment in any security, but only as an expression of Team8’s opinions. Team8’s statements and opinions are subject to change without notice. Team8 is not registered as an investment adviser under the Investment Advisers Act of 1940, as amended (the “Advisers Act”), and relies upon the “publishers’ exclusion” from the definition of investment adviser under Section 202(a)(11) of the Advisers Act. As such, the information contained in this Layer 8 - The Human Factor Article does not take into account any particular investment objectives, financial situation or needs and is not intended to be, and should not be construed in any manner whatsoever as, personalized investment advice. The information in this Layer 8 - The Human Factor Article is provided for informational and discussion purposes only and is

not intended to be, and shall not be regarded or construed as, a recommendation for a transaction or investment or financial, tax, investment or other advice of any kind by Team8. You should determine on your own whether you agree with the information contained in this Layer 8 - The Human Factor Article. Certain of the securities referenced in this Layer 8 - The Human Factor Article may currently, or from time to time, be constituents of an index developed and maintained by WisdomTree Investments, Inc. using data provided by Team8, which has been or will be licensed for a fee to one or more investment funds. In addition, certain officers or employees of Team8 or funds or other persons or entities affiliated or associated with Team8 may hold shares of, be officers or directors of, or otherwise be associated with some or all of the issuers of the securities referenced in this Layer 8 - The Human Factor Article or included in such index. Team8 expressly disclaims all liability with respect to any act or omission taken based on, and makes no warranty or representation regarding, any of the information included in this Layer 8 - The Human Factor Article.

[1] Source: https://www.wsj.com/articles/uber-says-it-is-victim-of-lapsus-a-hacking-group-motivated-by-fame-not-money-11663674367

[2] Source: https://www.nytimes.com/2022/11/04/technology/elon-musk-twitter-layoffs.html

[3] Source: https://www.nytimes.com/2022/11/09/technology/meta-layoffs-facebook.html

[4] Source: https://www.nytimes.com/2022/11/14/technology/amazon-layoffs.html

[5] Source: https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats#:~:text=Independently%20conducted%20by%20Ponemon%20Institute&text=Malicious%2C%20negligent%20and%20compromised%20users,a%20third%20to%20%2415.38%20million

Related blogs

+ In a bleak market for growth stocks, cybersecurity could be a future bright spot

+ Have you experienced ‘Tool Sprawl’ in Cybersecurity?

Important Risks Related to this Article

Important Information

Marketing communications issued in the European Economic Area ("EEA"): This document has been issued and approved by WisdomTree Ireland Limited, which is authorised and regulated by the Central Bank of Ireland.

Marketing communications issued in jurisdictions outside of the EEA: This document has been issued and approved by WisdomTree UK Limited, which is authorised and regulated by the United Kingdom Financial Conduct Authority.

WisdomTree Ireland Limited and WisdomTree UK Limited are each referred to as "WisdomTree" (as applicable). Our Conflicts of Interest Policy and Inventory are available on request.

For professional clients only. The information contained in this document is for your general information only and is neither an offer for sale nor a solicitation of an offer to buy securities or shares. This document should not be used as the basis for any investment decision. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. Any decision to invest should be based on the information contained in the appropriate prospectus and affer seeking independent investment, tax and legal advice.

The application of regulations and tax laws can offen lead to a number of different interpretations. Any views or opinions expressed in this communication represent the views of WisdomTree and should not be construed as regulatory, tax or legal advice. WisdomTree makes no warranty or representation as to the accuracy of any of the views or opinions expressed in this communication. Any decision to invest should be based on the information contained in the appropriate prospectus and affer seeking independent investment, tax and legal advice.

This document is not, and under no circumstances is to be construed as, an advertisement or any other step in furtherance of a public offering of shares or securities in the United States or any province or territory thereof. Neither this document nor any copy hereof should be taken, transmitted or distributed (directly or indirectly) into the United States.

Although WisdomTree endeavours to ensure the accuracy of the content in this document, WisdomTree does not warrant or guarantee its accuracy or correctness. Where WisdomTree has expressed its own opinions related to product or market activity, these views may change. Neither WisdomTree, nor any affiliate, nor any of their respective officers, directors, partners, or employees accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents.