ARTICLE

Is HEIST a Risk or a Threat?

Written by: Lori MacVittie

Date: August 12, 2016

Security professionals are tasked with understanding the difference between risks and threats and acting accordingly. To the layperson (that's most of us), the difference between the two may appear non-existent. After all, aren't they semantically equivalent? Don't we use them interchangeably to describe vulnerabilities and DDoS attacks and the latest zero-day exploit?

We might, but security pros are often a lot more precise than that, mostly because if they weren't, their budgets would outstrip all of IT as they waged a digital war against the growing stockpile of tools, techniques, and technology used to defeat their defenses. That's because not all threats carry the same risk.

Risk is a calculated measurement involving a number of factors including likelihood of occurrence and the impact if exploited. We all know that we could be hit by a bus and suffer dire consequences while crossing the road today, but the likelihood of that occurring is so low that most of us consider it a very low risk (if it even measures at all on our risk-meter). Conversely, wearing three-inch heels with no tread in the middle of a Wisconsin winter has a high likelihood of a fall occurring with unfavorable consequences, thus I personally consider that a pretty high risk in the winter months.

That's risk.

Threats are something else. Something else we can't control, like the weather or the bus routes or an attacker's decision to launch a volumetric attack on our website today.

One of the goals of security pros and their organizations is to minimize risk by mitigating threats and reducing likelihood of an exploit. If it's 20 below zero and the driveway is covered in ice, I wear flat, well-treaded boots. The threat is mitigated (but not eliminated) and thus risk is reduced. If a new vulnerability is suddenly discovered, I have to decide what risk that new threat poses to my organization.

EVERY
23 min
A WEBSITE IS HIT BY A CRITICAL EXPLOIT
(F5 Research)

In fact, this is so accepted as a methodology for assessing risk, the industry describes it mathematically:

A(sset) + V(ulnerability) + T(hreat) = R(isk)

This allows individual organizations to not only weight individual factors according to their business requirements and tolerance for risk, but act consistently. This can prevent panicked, knee-jerk reactions when new vulnerabilities are announced, particularly if the assessed risk turns out to be under organizational tolerances.

86%
OF WEBSITES HAVE AT LEAST 1 SERIOUS VULNERABILITY
WhiteHat Security Statistics Report 2015

So what about HEIST?

Which brings us to HEIST, which stands for HTTP Encrypted Information can be Stolen through TCP-Windows. HEIST is obviously much easier to say and sounds all Mission Impossible-like, doesn't it? This vulnerability was presented at BlackHat and is making its way around the Internet even now in articles at Ars Technica and Engadget. It has not, thus far, been sighted in the wild. It's not a simple vulnerability to exploit and researchers—including our own—note that it is not a trivial task to exploit HEIST. It's a complex side-channel attack that combines browser API behavior (it observes the way TCP normally works with a browser API that can time the responses), web application behavior, content compression, TCP, and SSL/TLS.

56
AVERAGE NUMBER OF VULNERABILITIES PER WEBSITE
WhiteHat Security Statistics Report 2015

This attack could be network heavy if multiple requests need be completed, but is better suited in the "noisy" category. Both are unattractive to bad actors who don't want to get noticed. And yet, if it is successfully exploited, attackers could combine it with BREACH or CRIME to decrypt payloads and hit the proverbial digital jackpot, exposing sensitive (perhaps critical) personal and

business data. In that case, they likely wouldn't care how noisy they were if they were successful in obtaining Personally Identifiable Information (PII)—the digital jackpot.

This is a threat. It could be used to exfiltrate data. That's called a breach and it's a Very Bad Thing™. The question is, when does this threat become a real risk?

Well, today (when I wrote this, to be precise), this threat was not existential. That is, it hadn't been seen in the wild. But that doesn't mean it isn't in the wild, it just means it hasn't been seen in the wild. Yet. Today. Right now.

Head spinning yet? Now you know why security pros always seem to have a dazed look on their faces. Because they have to manage this kind of thought process and decision making all the time.

So the question becomes if this threat becomes existential, what is the risk? To answer that, you have to determine what the impact would be if the vulnerability were exploited. If someone manages to exfiltrate data from your app, your site, what's the impact? What's your cost going to be? Don't forget to include brand impact, that's part of the (increasingly complex) equation. So is the cost of mitigation. The equation changes when the cost of mitigation is high versus a relatively low impact solution. If you have to touch every web server in the data center (and in the cloud) to twiddle just a single setting to mitigate the threat, that's a lot of time (and subsequently money) for something that might could be existentially threatening. If the risk is low, you'd likely adopt an understandable "wait and see" attitude rather than scramble because the boy cried "wolf."

If the mitigation is relatively low impact in terms of costs to implement, say a simple script that confuses the attacker by varying the size of data returned and thus making HEIST more difficult to carry out, you might consider moving ahead and putting it into place. After all, the cost of lowering risk even further was minimal, and it's almost certainly far less than the consequences if said HEIST is carried out in the future.

A Constant (Re)balancing Act

The reality is that security is a constant battle to minimize risk by mitigating threats while wading through the political minefield that is most IT organizations. Too often security pros decide against the effort to implement even simple mitigations for threats with fluctuating likelihood of risk because

IT exists in silos of functionality. They wait until the risk rises and forces a reaction, rather than proactively mitigating the threat. For example, many of the most talked about exploits of the past two years were application focused. To mitigate them, solutions need to be deployed in the data path, upstream from the application, because the most efficient and effective location to do so remains the point at which applications are ultimately aggregated for scale and delivery. But that strategic point of control is managed by application delivery teams, not security teams. The effort required to mitigate such threats early on outweighs the risk. Because the ability of the two groups to meet in the middle, as it were, remains a constant challenge for organizations, proactively reducing risks and mitigating threats at the application layer simply does not happen.

HEIST is, right now, likely considered a low risk for most organizations. But make no mistake, it is a threat, and thus deserves consideration now, when we've all been given notice as to its existence before it's put into play. Cross-coordination is required, so that "serverless" security solutions like this mitigation for HEIST can be deployed before the threat becomes existential and the risk of exploitation drives everyone into a frenzy of costly activities and implementations to address it.

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com