THREAT SCORING

A qualitative and quantitative approach to consistent threat evaluation

The following matrix is used to provide a quantifiable threat score based on the threat actor and target characteristics. To make the overall threat score compatible with current industry standards for vulnerability scoring, the Overall Threat Score should be multiplied by 10, then added to the residual risk score for a CVSS vulnerability. To determine how to calculate residual risk from a raw CVSS score visit https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Please send your questions to the author, Tazz 447cc8c9 \at\ opayq.com

THREAT ACTOR IMPACT SCORING						
	1	2	3	4	5	SCORE
1. Determination	Timid, scares easily, afraid to go to jail, will disengage completely	Passive, will go dormant engaged	Assertive, willing to commit non-interactive fraud, lie, steal (ex: phishing)	Aggressive, will interact in-person or remote, to exploit victims (ex: social engineering)	Hostile, highly confident, undeterred by legal/political consequences	
2. Motivation	Bragging Rights	Incentive / Coercion	Monetary Gain	Induce Change	Power / Destruction	
3. Resources: Technical	Free Only, publicly available	Free / Inexpensive (relative to income) & widely available	Combination of Paid & Widely Available, Customizable with some in-house development	In-house developed, invite-only purchases OR found in underground markets	Restricted development (for profit 0-days or govt-only use)	
4. Funds Avail.	$0-$2,000	<$10,000	<$50,000	<$2M	$2M+	
5. Resources: Intelligence	Open Source Only	Internal Company Tactical	Internal Company Operational	Internal Company Strategic	Internal, Proprietary or Government	
6. Skills & Experience	Low Skill/Experience – never executed a campaign	Average – can execute a small campaign – lots of forensics evidence	Experienced with comprehensive recon, has executed hands-on attacks before, moderate amount of forensics	Advanced – can customize an attack in advance – minimal forensic footprints	Experts – can pivot and customize on the fly – leaves little to no forensics	
7. Time Undetected	None	<30days	31-180 days	6-12 months	1 year+	
8. Team Size	<5 part-time non-tech savvy	<10 part-time Non-tech, or 1-4 tech savvy	>10 Part Time Non-tech, or 5+ Part time tech savvy	Full Time, 10+ tech experts	20+ tech experts	
9. Time	5-15hrs/wk	15-30hrs/wk	30-40hrs/wk	40-80 hrs/wk	24/7 coverage	
					RAW TOTAL A	

THREAT TARGET SCORE						
	1	2	3	4	5	TREAT SCORE
Probability of Successful Actor Attack	Highly unlikely	Unlikely	Somewhat Likely	Likely	Highly Likely	
Technical Exploit	No concept, No indicators	Concept Exists, but No Exploit	Exploit Exists	Exploit is in the Wild, but not organic	Peers/Clients Exploited	
Non-Technical (Attack Focus)	No specific focus (Spray & Pay)	Non-USA focused	USA-focused	Tech-Industry Focused	$my_org/Peer/Customer Focused	
					RAW TOTAL B	

Threat Actor Impact Score (Raw Total A)	A	Out of 45	
Threat Target Score (Raw Total B)	+ B	Out of 15	
Overall Threat Score	= C	Divided by 60 =	D

Overall Threat Score	(D * 10)
Overall CVSS Score (Raw CVSS after mitigation)	+ CVSS RR
Overall Risk Score	#.#