Vulnerability Intelligence: What's the Word in Dark Web Forums?

digitalshadows.com/blog-and-research/vulnerability-intelligence-whats-the-word-in-dark-web-forums/

November 16, 2021

Note: This blog is part of a three-blog series on Vulnerability Intelligence that accompanies the release of Digital Shadows' latest whitepaper titled Vulnerability Intelligence: Do You Know Where Your Flaws Are?

Managing vulnerabilities is a daunting task for security teams that are constantly busy with keeping up with the vulnerability threat landscape. New security flaws are discovered every day; consequently, security teams are often pushed into patching without adequate planning and missing bugs that continue to represent a significant risk. The result? Cybercriminals and state-sponsored threat actors can often leverage unpatched vulnerabilities to get access to a target's environment and conduct further malicious activity.

In an ideal world, these vulnerabilities are responsibly disclosed, giving vendors time to respond publicly and roll out timely patches. Even better, critical software vulnerabilities would get patched automatically! In this utopian environment, patches wouldn't cause everything to break in production and conflicting interdependencies could be easily fixed. Doesn't this sound dreamy? Sadly, this is not a very plausible scenario for most security teams out there.

We won't judge you if you plan on turning into a Metapod when faced with patching dilemmas

The current information technology (IT) landscape is a highly complex environment of old and new technologies that have significantly expanded the attack surface. When new vulnerabilities are disclosed, security teams often need to scramble to figure out how these would impact their systems and what to patch first. Adopting an efficient vulnerability management program can offset some of the traditional challenges associated with triaging threats and asset management, and significantly improve your organization's security posture.

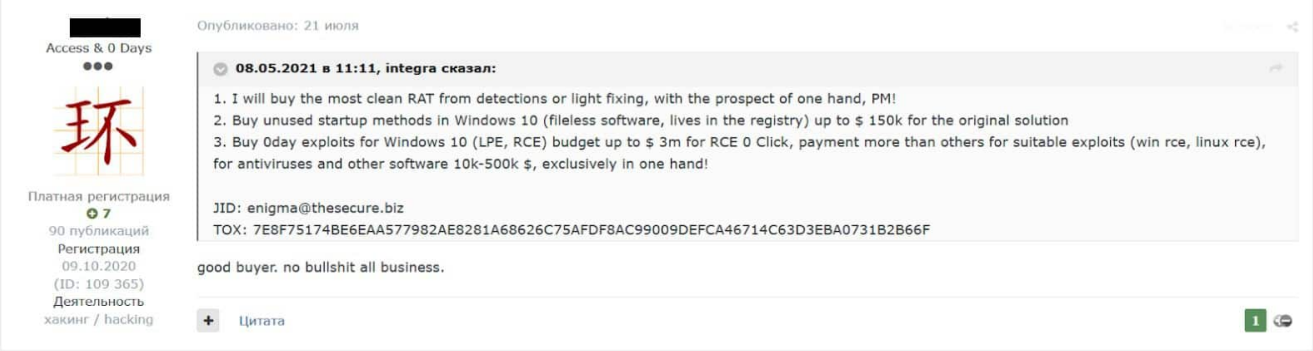
For this reason, Digital Shadows has just published its latest research piece titled *Vulnerability Intelligence: Do you know where your flaws are?*, where we have explored the cybercriminal forums rabbit hole to understand how threat actors are continually exploiting

security teams' weaknesses. The picture we obtained has convinced us that the traditional – and sometimes chaotic – approach to vulnerability patching is not sustainable anymore and that we need a new paradigm to stay one step ahead of malicious actors.

What Does the Illegal Zero-Day Market Look Like?

As part of our investigation, we gathered extensive primary source evidence from cybercriminal markets and forums to better comprehend how the vulnerability criminal industry looks. This environment is bursting with a variety of widespread actors who boast a whole range of technical expertise and motives. The technical discussions of this eclectic underground cohort have actually contributed to a pretty cohesive, crowd-sourced body of knowledge about vulnerabilities and exploits.

The top of the cybercriminal pyramid is represented by the market for zero-days. This market is an extremely expensive and competitive one, and it's usually been a prerogative of state-sponsored threat groups. However, certain high-profile cybercriminal groups (read: ransomware gangs) have amassed incredible fortunes in the past years and can now compete with the traditional buyers of zero-day exploits.



Threat actor offering 3,000,000 USD for a 0-click RCE zero-day

This is probably why zero-day sellers have moved their auctions to cybercriminal forums: to fish in this large and wealthy pool. Zero-day exploits are incredibly pricey and we've observed threat actors claiming that they could go away for up to $10,000,000. These prices may look jaw-dropping but there's a key aspect to keep in mind. Whatever legitimate bug bounty programs offer, cybercriminals must offer more in order to compete with them, given the risks (jail time) and additional requirements needed during illicit activity (i.e. money laundering).

Is it clear now why this has traditionally been a state-sponsor-exclusive club? Very few cybercriminals have that kind of money to splash on a vulnerability. And even fewer of them will be actually motivated to invest that sum when organizations still have public-facing remote desktop protocol (RDP) appliances in their networks (and yes, there are a lot of them). But an espionage campaign of a state-sponsored APT group can easily justify sinking funds into an exclusive zero-day, if it reels in invaluable information.

The Rise of the Exploit-as-a-Service Model?

Feel like a multi-million dollar price tag may be a bit too much for your pockets? No worries, the cybercriminal community doesn't leave anyone behind to miss out on all the zero-day fun! During our investigation for this research piece we've noticed cybercriminals discussing ideas for an Exploit-as-a-Service business model that would inevitably lower the barrier for accessing sophisticated exploits.

This model would allow capable threat actors to "lease" zero-day exploits to other cybercriminals to conduct their attacks. In fact, while a developer can generate large profits when selling a zero-day exploit, it often takes them a significant amount of time to complete such a sale. However, this model would enable zero-day developers to generate substantial earnings by renting the zero-day out while waiting for a definitive buyer. Additionally, renting parties could test the proposed zero-day and later decide whether to purchase the exploit on an exclusive or non-exclusive basis.

Zero-day exploit developers can certainly generate large profits by selling to government-backed threat actors, but this process can eat up time and drive the developers to seek alternative revenue sources. And that's when exploit-as-a-service becomes viable—generating their desired income from various interested parties. The result? More and more financially motivated threat actors with their hands on dangerous tools.

Old Vulnerabilities Are Still a Serious Problem

Zero-days and high-profile threat actors can certainly make up for great insights into the cybercriminal world but they do only represent a tiny fraction of this complex ecosystem. The wide majority of the cybercriminal community is in fact busy discussing and sharing knowledge on older vulnerabilities that security teams haven't properly patched yet.

Apart from a few exceptions, the cybercriminal community is known for being opportunistic and targeting the low-hanging fruit rather than mounting highly-sophisticated offensive campaigns. Overlooked security flaws in software and hardware may well provide cybercriminals with valuable initial access to a victim's environment and cause some serious harm from there.

Nothing will ever hurt more

The user base for older vulnerabilities is broad. For starters, many low-skilled cybercriminals need some time before they can exploit a new vulnerability, and maybe even need support from the cybercriminal community, like tutorials or guides on how to use the latest exploit. Then there are the penny-pinchers. Despite the high payouts associated with cybercrime, we're all now aware that the best (zero-day) exploits don't come cheap. It can be worthwhile to wait for a vulnerability to become more mainstream, with corresponding PoCs or exploits released for free or at a lower price.

Strengthen your Fortress with Vulnerability Intelligence

Ok, maybe the ideal world described at the beginning of this blog is still far away from our radar. However, security teams can still significantly improve their security posture with a few changes to their habits. For example, incorporating a risk-based approach to vulnerability management can go a long way in helping security teams navigate this sea of vulnerabilities. A framework based on the impact and likelihood of vulnerability exploitation can certainly help mitigate some of the triaging and asset management challenges mentioned above.

However, making informed decisions requires a good dose of contextual knowledge around the latest vulnerabilities disclosed. Identifying intelligence needs based on your threat model is therefore crucial to improve triaging and patching processes. Incorporating vulnerability intelligence will help you prevent and quickly mitigate the most relevant threats for your specific organization. And once fused into your organization's threat model, vulnerability

intelligence can be used across a variety of internal functions to improve security planning, such as triaging threats, communicating them across the board, and mitigating them in a timely and accurate manner.

Want to hear more about it? Download our free Vulnerability Intelligence report here!

Tags: forums / photon research team / vulnerability intelligence