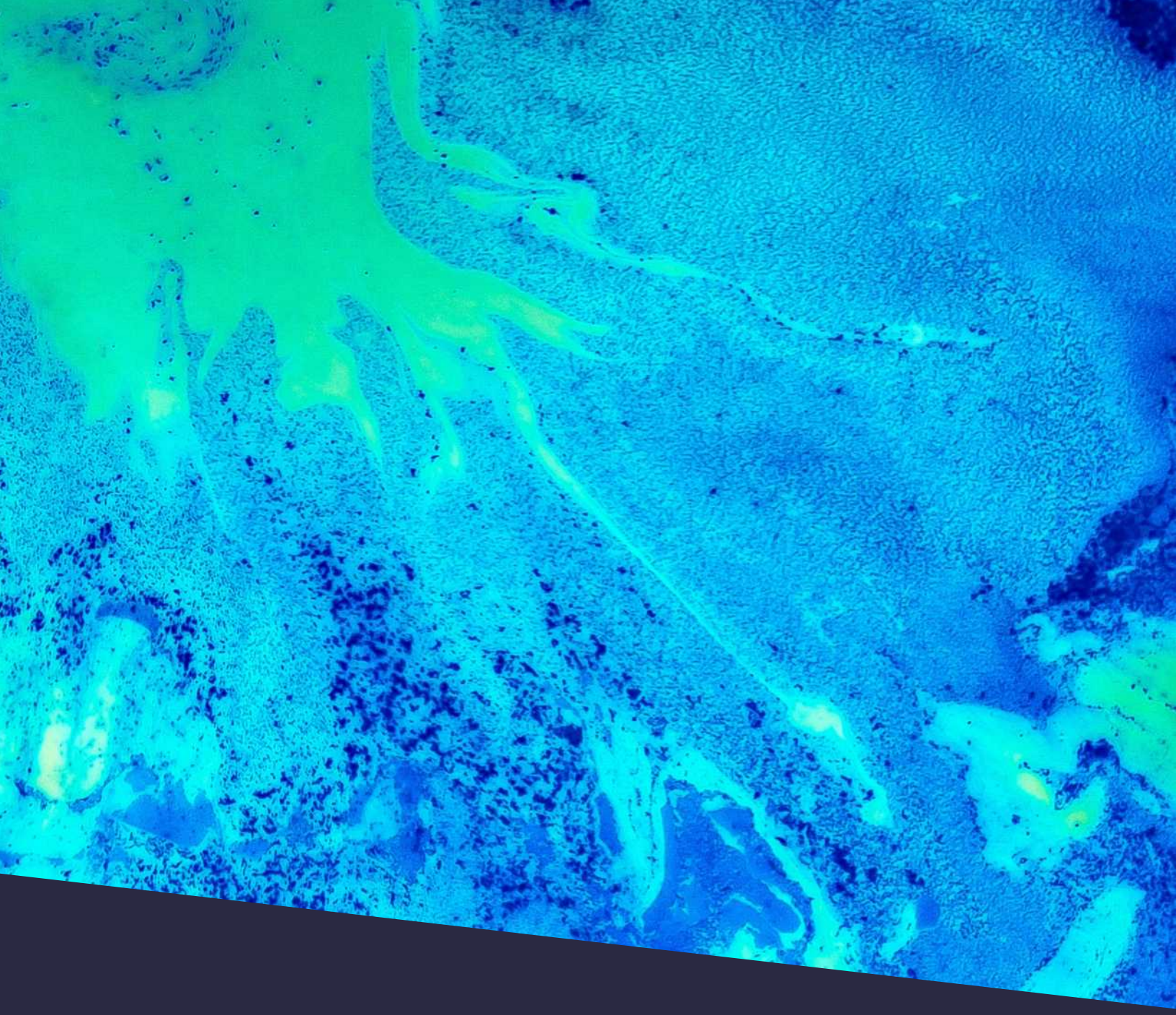


VULNERABILITY INTELLIGENCE:

DO YOU KNOW WHERE YOUR FLAWS ARE?

Digital Shadows Research Team

digital shadows_

VULNERABILITY INTELLIGENCE: DO YOU KNOW WHERE YOUR FLAWS ARE?

EXECUTIVE SUMMARY

Have you ever had this nightmare: You show up to work as the cyber-security manager of a prominent company, and you take a look around… the building, the networks, the cloud. You see legacy infrastructure—old IT equipment still in use—sitting alongside the latest technology. They're entangled; a mess, really. Your team hands you a list of software and hardware vulnerabilities they think you should worry about, pages long. Then the executives hand you a list of vulnerabilities they think you should worry about. They're different lists. Your heart pounds. *What should we patch?! Are there even patches available?* Then you notice the clock: It's 5 pm.

Managing vulnerabilities is a daunting task in an increasingly nightmarish world. With new vulnerabilities discovered every day, security teams are pushed into patching without adequate planning, or missing bugs that continue to represent a significant risk. We're still not doing enough to fight what's really the most basic of problems for any security team.

Digital Shadows' Photon Research Team has researched the patching challenges faced by security professionals across almost every organization. Down the rabbit hole of cybercriminal forums, we came to understand how threat actors are continually exploiting security teams' weaknesses. The traditional, sometimes chaotic approach to vulnerability patching is not sustainable anymore.

Here are the top discoveries from our research:

- **Threat actors are working tirelessly to exploit neglected vulnerabilities for their attacks.**
- **Proof of concept (PoC) code exposed by security researchers has been exploited by opportunistic threat actors. Monitoring for relevant Indicators of Compromise (IOCs) can help preemptively mitigate risks to your organization.**
- **Zero-day vulnerabilities, unaffectionately known as zero-days, are the most expensive flaws advertised on cybercriminal forums—unsurprisingly. Digital Shadows has observed cybercriminals discussing zero-days prices and reaching up to USD 10,000,000 during this investigation. If these prices once were a prerogative of exclusively state-sponsored threat actors; now cybercriminals have amassed sufficient fortunes to compete with them.**
- **Older (and overlooked) vulnerabilities remain highly valuable to cybercriminals. They provide a cheap and efficient entry point into target environments. Low-skilled threat actors can easily exploit these flaws, carrying out attacks by relying on premade tools and methods provided by their more experienced counterparts.**
- **Both expert and novice cybercriminals often cooperate and share knowledge to enhance their exploitation skills and carry out disruptive attacks.**
- **Information overload, absence of vision of internal assets, and problems effectively communicating risks and liabilities to executives are only some of the obstacles that hinder an effective patch management process.**
- **A risk-based approach is an effective defense to vulnerability management; it considers risk and likelihood of an exploit when dealing with the enormous amount of flaws out there. Vulnerability intelligence helps by favoring a proactive security posture and support in triaging, understanding, and mitigating flaws.**

THE TRADITIONAL, SOMETIMES CHAOTIC APPROACH TO VULNERABILITY PATCHING IS NOT SUSTAINABLE ANYMORE.

1. PATCHING CRISIS: ADMITTING THE PROBLEM, FINDING THE CURE

1.1 A FLAWLESS WORLD (AS IMAGINED BY A SECURITY DEFENDER)

Picture a world where software code never presented any problems. Or let's say it did, but any vulnerabilities in the code were responsibly disclosed, giving vendors time to respond publicly and roll out timely patches. Zero days don't exist! Updates simply show up in any device or solution that requires them! And maybe, in this perfect world, the software even just *updates itself*.

The consequences for security teams in that world would be unprecedented. Patches wouldn't need days or weeks of testing, because there aren't interdependencies that break everything in production once rolled out. Best of all, the bad guys would realize that targeting critical network infrastructure is not in society's best interest…they would stop exploiting vulnerabilities and trying to monetize security lapses. Security managers would take Fridays off, and throw out their blood pressure medication.

Unfortunately, that's not the world we live in. Because humans write code, inevitably there will be errors. Operating systems and applications have grown more complex, and there is always likely to be a problem buried in the thousands to millions of lines of code.

Plus, there's the patching problem. Sure, patches are available, but who's around to actually put in the work of updating to the latest software versions? Will it break the other applications and systems already installed? What unforeseen problems may arise for the user once updates are rolled out? And how to even prioritize: Which patches are the most critical?

After a vulnerability is announced, adversaries everywhere look to take advantage by either weaponizing a PoC or developing their own exploits. Experience has taught them that, despite a lot of companies proactively managing vulnerabilities, there are always a few that don't patch, or patch too slowly: ideal for opportunistic attacks. Also, let's face it, attackers may get lucky and land amid a company's crown jewels.

1.2 OUR FLAWED WORLD—PATCHY, AT BEST

As the past decade has seen the information technology (IT) landscape evolve into a highly complex environment of old and new technology, securing organizations' networks and servers has become about dealing with a variety of hardware and software, locations and vulnerability types.

An effective vulnerability management (VM) program can lower cyber risk. However, many organizations with such a program in place still encounter significant problems in remediating security flaws. A lack of resources, unclear roles and responsibilities, and absence of managerial approval for effective change can leave VM in a deficient state.

The ongoing COVID-19 pandemic has also placed more strain on information security professionals, with millions of workers adapting to partially or fully remote roles. Many cyber-security budgets have also been pushed to the brink, even as the cyber-threat landscape changes dramatically.

Let's try to figure out where the real problems lie, to steer your VM program on the right course.

1.2.1 FALLING SHORT IN TRIAGING THREATS

One of the major problems with VM is inability or inconsistency when triaging exposures. Maybe you're following advice to perform discovery of assets, assess and scan them for risks, and create a report before you attempt remediation and verify results. Those efforts suck time and resources away from accurate triage, leaving a mountain of issues to fix and no real plan of action. VM is neverending, and no matter how many bugs are fixed, more will surface. Triaging flaws—by identifying those with the potential to cause the biggest problem—and fixing them first should be the primary consideration of any VM team.

The factors that need to be considered for triage vary widely for each organization but, generally speaking, they're:

- **Whether a vulnerability has been exploited**
- **Whether a working PoC exploit is available in an open source**
- **The impact that can be caused by successful exploitation**

The latter is typically determined by considering which assets are affected by the vulnerability and their overall role. For example, a medium-severity vulnerability that is exploitable and external facing should be prioritized over a critical vulnerability that has a limited chance of being targeted by attackers.

1.2.2 POOR ASSET MANAGEMENT: FAILURE TO PREPARE IS PREPARING TO FAIL

Another core problem is that many organizations have an uncoordinated VM program. Although highly dependent on an organization's size, resources, and structure, patching efforts are ideally coordinated by a single entity or department. Having multiple units all running their own efforts to remediate vulnerabilities can lead to flaws not being processed consistently. This can lead to certain parts of the business being prioritized or remediated at different levels. Or bugs can pile up as issues go unfixed, and that kind of 'tipping point' can mean significant problems.

The VM team should understand the organization's architecture—and have a complete asset inventory of equipment, hardware, software, and services being used—so problems are immediately spotted. In theory, they should also be tracking the lifecycle of every organizational asset: from the day it's purchased to the day it's retired.

But organizations are continually changing, which is why management support is absolutely essential for VM to make risk-lowering changes. The VM team should mandate notification of all architectural shifts, mergers, acquisitions, new servers, and the like. Failure to do so can leave unknown vulnerabilities in blind spots on your network…basically, open doors for threat actors to slip through. You can't defend what you don't know you have.

VM teams are likely to encounter several problems, notably resistance to update devices: because the risk is sometimes deemed acceptable, because backups exist, or because patches are regarded as untrustworthy or unnecessary. Buggy patches often do cause problems—which is why local testing and the manager-level support are critical for a VM team to approve and enforce changes in the face of resistance from local administrators or system owners.

ELIMINATING JUST THE EXPLOITABLE VULNERABILITIES—EVEN IF THEY ONLY REPRESENT A SMALL FRACTION OF THE TOTAL IDENTIFIED VULNERABILITIES—CAN SEND CYBER RISK PLUMMETING.

1.3 THE FUTURE WORLD: PROACTIVE VULNERABILITY MANAGEMENT

Security teams can be slow and inaccurate when responding to vulnerabilities for a variety of reasons—we've already lamented about ineffective triage processes, and don't even get us started on outdated corporate policies. There are hundreds of obstacles in the way of a great VM program, and threat actors are well aware of that. Don't expect empathy when they see the potential for compromise; many of these threat actors are opportunistic—show them an open door and they'll happily step inside.

Your best line of defense in the face of all this adversity is an effective VM and intelligence program that reflects a proactive (rather than reactive) security posture. Trust us, your incident responders will thank you for it, and so will the execs.

Without further ado, we present three major areas for security teams to focus their VM on:

1. **The steps that lead to vulnerability exploitation and attack**
2. **The top five vulnerabilities observed by the US Cybersecurity and Infrastructure Security Agency (CISA) in the first half of 2021**
3. **Trends and major players in the exploitation community**

In the following sections devoted to each area, we've planted a red flag next to each factor you should consider carefully when implementing a VM strategy. 🚩

2. ATTACKERS, THIS WAY: THE EASY ROUTE TO EXPLOITATION

Knowing what to look for is the first and most important step for any security analyst. In this case, we're talking about two critical steps that propel a simple vulnerability disclosure into a fully fledged cyber attack. Monitoring for 1) premature releases of PoCs and 2) activity related to vulnerability scanning on the Internet can go a long way in VM, by helping you identify and prioritize the most impactful security flaws, quickly and accurately. Full disclosure: looking for these signals when they're already out in the wild means having a reactive security posture, and we've already acknowledged that's historically caused severe issues. But regardless, both steps should be major points of interest for any security team, factored into your VM program.

2.1 VULNERABILITY DISCLOSURE AND PROOF OF CONCEPT PUBLICATION

In information security, a PoC is an attack method used to demonstrate how a vulnerability can be exploited. Researchers may publish their recently developed PoCs in code-sharing repositories,on video-streaming platforms, in personal or security vendors' blogs, etc.

Security researchers typically develop PoCs to highlight a security flaw and urge the responsible company to patch it quickly. With a technical demonstration of how an adversary can exploit it, these researchers can significantly speed up the patching process. As a bonus, they're providing a useful benchmark for testing a patch before it's rolled out to the public.

In some other instances, researchers may be asked to provide a PoC to showcase the severity of a new flaw when disclosing it as part of a bug bounty program.[1] Or researchers may be trying to boost their status as a red-teaming[2] expert in the security community, by being among the first to provide a PoC for a newly discovered vulnerability.

PoC code may be intended for these good-spirited pursuits, and they're harmless when used as such. But when PoCs aren't disclosed responsibly, 🚩 and via the appropriate channels, 🚩 they can cause serious harm to users and companies alike—inviting more damage than security.

2.1.1 TO WAIT OR NOT TO WAIT: THE POC DEBATE

Publishing PoCs before the effective patching of a vulnerability for all users has often inflicted a world of pain. The controversial when-to-publish debate has split the security community in two factions that exchange incendiary dialogue at every security conference. Here's what they argue:

Argument 1: PoCs are often necessary to push the responsible company to adequately patch their software quickly and efficiently. Disclosing a vulnerability via private channels may not sufficiently motivate them to act immediately, giving attackers time to discover and exploit that flaw. But that's not all! (They claim.) A PoC allows organizations using the vulnerable software to independently check whether their systems are exploitable, which makes potential victims more resilient: They can better understand the scale and severity of the issue, and make more informed decisions about remediation.

Argument 2: The premature publication of PoCs have often caused more harm than good, and contribute to an unstable threat landscape (see the Case Study below for a real-life worst-case scenario). Although state-sponsored and highly skilled threat actors can reverse-engineer available patches and create working exploits from them, their job is made much easier by freely available PoCs for new or undisclosed vulnerabilities. And even the technically unsophisticated actors benefit, by using that public PoC to test their skills against vulnerable software. And if that doesn't sway you, consider that the publication of a PoC has often led to quick exploitation—within hours or days—without ample time for security teams to adequately patch their systems.

So there you have it. Two factions, and each makes a good case. Being mindful about timeliness and transparency are key to a secure disclosure of a PoC and will ultimately increase the chance of a positive impact.

[1] A bug bounty program is a deal offered by many websites, organizations and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities.

[2] Red teaming is the act of systematically and ethically using real-world offensive techniques to breach an organization's security defense in order to anticipate the attackers' moves.

Timeline of Citrix CVE-2019-19781 exploitation

CASE STUDY: THE PREMATURE PUBLICATION OF CVE-2019-19781

Spoiler alert: If you're looking for a happy ending, this story doesn't end well for all involved. It starts on 17 Dec 2019, when Citrix disclosed a directory traversal vulnerability in the Citrix Application Discovery Controller and Citrix Gateway. It was designated CVE-2019-19781 (according to a dictionary of publicly disclosed cyber-security vulnerabilities and exposures whose entries comprise an identification number, a description, and at least one public reference). The flaw could enable a remote, unauthenticated attacker to perform an arbitrary remote code execution (RCE) without the need to provide authentication credentials for a device.

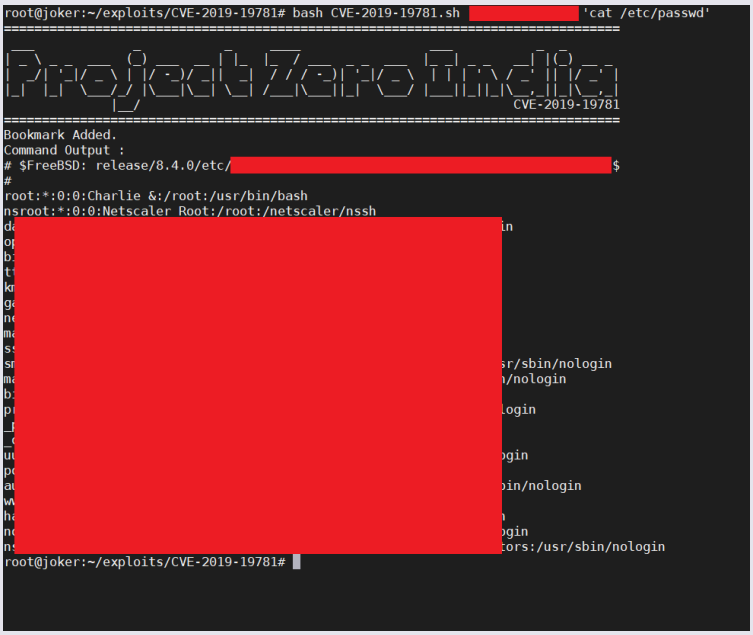
This dangerous little flaw (CVSS score: 9.8, rating: Critical, reaction: yikes) wasn't patched immediately. Instead, Citrix published an advisory for temporary mitigation and a road map for the upcoming patch. In the meantime, security researchers started claiming they could weaponize CVE-2019-19781, but said they would avoid disclosing technical details until the patch was made available. On this occasion, the security community seemed unanimous in the view that the flaw's severity, and the wide adoption of the vulnerable software, required everyone to cooperate and advocate for mitigation.

Well, it wasn't long before someone published a working PoC. On 10 Jan 2020, the code appeared on GitHub, which triggered several red-teaming professionals to release their own exploits, as well. Now there were multiple pieces of security-flaw code flying freely through the Internet, available for even low-skilled threat actors to use.

The result? As you'd expect: On 11 Jan 2020, multiple threat actors began weaponizing the public PoC and attacking Citrix servers worldwide. The popularity of this Citrix software made it an absolute favorite for malicious actors, and they relished the arbitrary code execution—using it to gain administrator rights to a machine proved extremely popular.

Citrix ultimately published a patch on 20 Jan 2020. Although it worked just fine for organizations that hadn't been targeted already; for compromised systems, attackers could maintain their access even if the patch was applied.

The precipitous publication of the working PoC ultimately escalated the threat of this vulnerability. If security researchers had waited for Citrix to patch the software, the risk of attack would probably have been much lower.



The first publicly available PoC exploit code for CVE-2019-19781 (Source: GitHub)

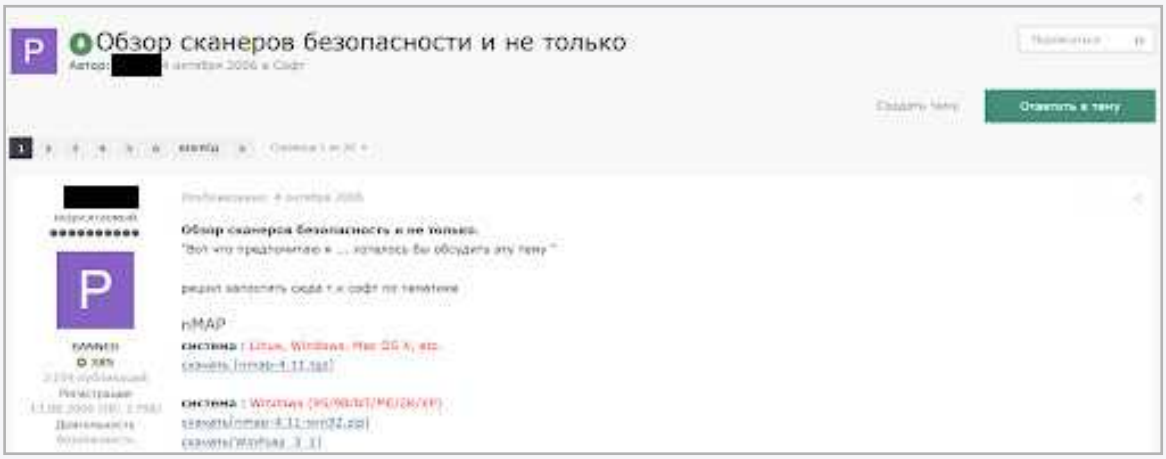
English-language cybercriminal forum user advertises SQLI Vulnerability Scanner

2.2 SCANNING THE INTERNET FOR VULNERABLE ASSETS

Usually in the wake of a vulnerability disclosure—and almost assuredly after exploit disclosure—security teams everywhere are the first to feel the effects of mass Internet scanning. It may be from other security firms conducting research, but it's also the work of adversaries, sniffing around for vulnerable points in networks. Whether they're using a Nessus, OpenVAS, Nmap, zMeU, Acunetix, Qualys, or similar vulnerability scanner, they make the Internet come alive when exploits are announced.

In these instances, because of the sheer volume of scans and exploit attempts, it can be incredibly difficult (if not nearly impossible) to know who's scanning or why. Unless scans are coming from a known ASV (Approved Scanning Vendor) or an otherwise known, "allowlisted" appliance, you'll probably never know. But rest assured: Threat actors are definitely at work in these scenarios; they never miss a chance to scan vulnerable products that might aid a cyber attack.

Opportunistic cybercriminals frequently use scanners to spot as many vulnerable products as possible, then exploit them during malicious campaigns. And for years they've discussed the best vulnerability-scanning tools, on cybercriminal forums and marketplaces. One of the most popular threads on the Russian-language cybercriminal forum Exploit dates back to 2006: Users reviewed vulnerability scanners and shared "cracked" versions of paid penetration testing tools.



Example of a cybercriminal reviewing vulnerability-scanning tools from 2006

Example of a cybercriminal suggesting scanners popular for targeted attacks

Novice threat actors can "jump start" their cybercrime careers by using vulnerability-scanning tools; from there, they learn how to manually detect vulnerabilities, how to exploit them, and, ultimately, how to write their own exploits. They can also find out, from other cybercriminals, how to use scanners to gain initial network access. The cybercriminal community supports "newbies" who are eager to learn more about the tradecraft, and we've often seen them providing detailed reviews of the most suitable tools out there.

2.3 GREATEST HITS OF 2021: TOP 5 VULNERABILITIES EXPLOITED

On the Photon Research Team, we're big threat intelligence nerds, and we firmly believe in a proactive security posture. Being aware of what's happening out there—and able to place it in the right informative context—builds the knowledge body required for informed decisions. We're constantly examining the most exploited vulnerabilities in the wild to better understand threats and threat actors' TTPs (tactics, techniques, and procedures).

In this section you can reap the rewards of our proactive diligence by learning about the top 5 vulnerabilities exploited in the wild in 2021, as observed by key cyber-security institutions. (See the security advisory published by CISA and coauthored with the Australian Cyber Security Centre (ACSC), the UK National Cyber Security Centre (NCSC), and the US Federal Bureau of Investigation (FBI).

These five vulnerabilities are a great study resource. For starters, they're relevant right now. And they represent a good sample of zero-day vulnerabilities and older, neglected flaws. They also affect a range of day-to-day software and hardware that many organizations frequently use. Finally, behind their exploitation are threat actors a grab bag of motives and capabilities, giving you a balanced overview of what's possible out there. (It's not pretty.)

TOP 5 VULNERABILITIES EXPLOITED BY THREAT ACTORS IN 2021

PRODUCT	CVE	CVSS SCORE
Microsoft Exchange	CVE-2021-26855 CVE-2021-26857 CVE-2021-26858 CVE-2021-27065	9.1
Pulse Secure	CVE-2021-22893 CVE-2021-22894 CVE-2021-22899 CVE-2021-22900	10.0
Accellion	CVE-2021-27101 CVE-2021-27102 CVE-2021-27103 CVE-2021-27104	9.8
VMWare	CVE-2021-26985	9.8
Fortinet	CVE-2018-13379 CVE-2020-12812 CVE-2019-5591	9.8

Source: CISA

MS EXCHANGE SERVER	
CVEs	CVE-2021-26855 CVE-2021-26857 CVE-2021-26858 CVE-2021-27065
Zero-Day	Yes
Threat Actors	HAFNIUM (APT) REvil (Ransomware) DearCry (Ransomware) Black Kingdom (Ransomware) LemonDuck (CryptoJacker)

PROXYLOGON AND THE POC DILEMMA

On 10 Mar 2021, a security researcher published the first ProxyLogon PoC on GitHub: a largely working RCE exploit that needed only minor tweaks. A few hours later, Microsoft-owned GitHub took that repository down for security reasons. As it happens, despite Microsoft having already provided a patch, more than 50,000 servers remained unpatched at the time. This takedown ignited a heated debate in the security community and forced GitHub to review its exploit-hosting policy and provide more transparency for future instances.

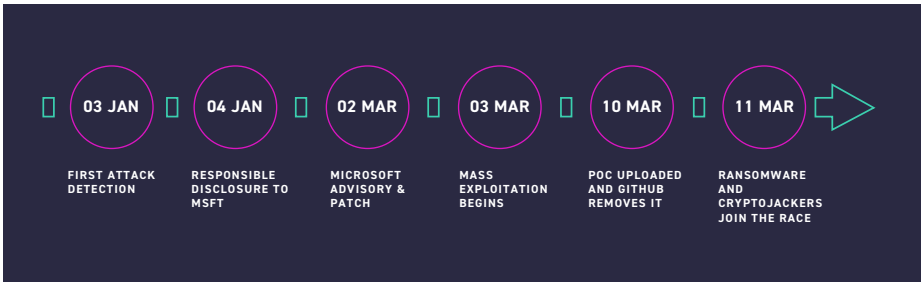
2.3.1 STATE SPONSORSHIP, RANSOMWARE, AND CRYPTOJACKING

On 02 Mar 2021, Microsoft released an advisory about multiple zero-days collectively known as ProxyLogon (individually, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065). They were used to compromise on-premise versions of Microsoft Exchange Server, a calendar and collaboration platform designed for business use.

That same day, Microsoft attributed, with high confidence, the first wave of attacks to "HAFNIUM", an espionage group believed to be supported by and operating from the People's Republic of China (PRC). This advanced persistent threat (APT) group primarily targets various industries in the US, such as think tanks, infectious-disease researchers, defense contractors, and educational institutions, to exfiltrate information.

Microsoft quickly issued patches for the vulnerabilities but warned its customers that they may remain vulnerable to attacks if previously targeted. Additionally, Microsoft released a script that would allow its customers to check for IOCs attributed to HAFNIUM, and warned that attacks would also likely emanate from other threat groups. But with this public acknowledgment of ProxyLogon, more threat actors were inspired to learn about it… and so the mass exploitation began.

State-sponsored threat groups were the first to target ProxyLogon *en masse*, as early as mid-March. A week after Microsoft's advisory, security researchers observed exploitation by more than ten, and many were linked to the PRC. Other threat groups quickly followed, including ransomware operators and cryptojackers[3]—ransomware operators are traditionally flexible and quick to adapt to new exploitation opportunities. The "DearCry", "Black Kingdom", and "REvil" groups all used ProxyLogon to deploy their ransomware in vulnerable environments. Around the same time, researchers detected attacks using web-shells deployed on compromised servers to download malicious payloads associated with the "LemonDuck" cryptojacking botnet.



Timeline of ProxyLogon exploitation

[3] Cryptojackers are threat actors who use a victim's device to mine cryptocurrency without their permission or knowledge.

2.3.2 APTS AND ZERO-DAYS

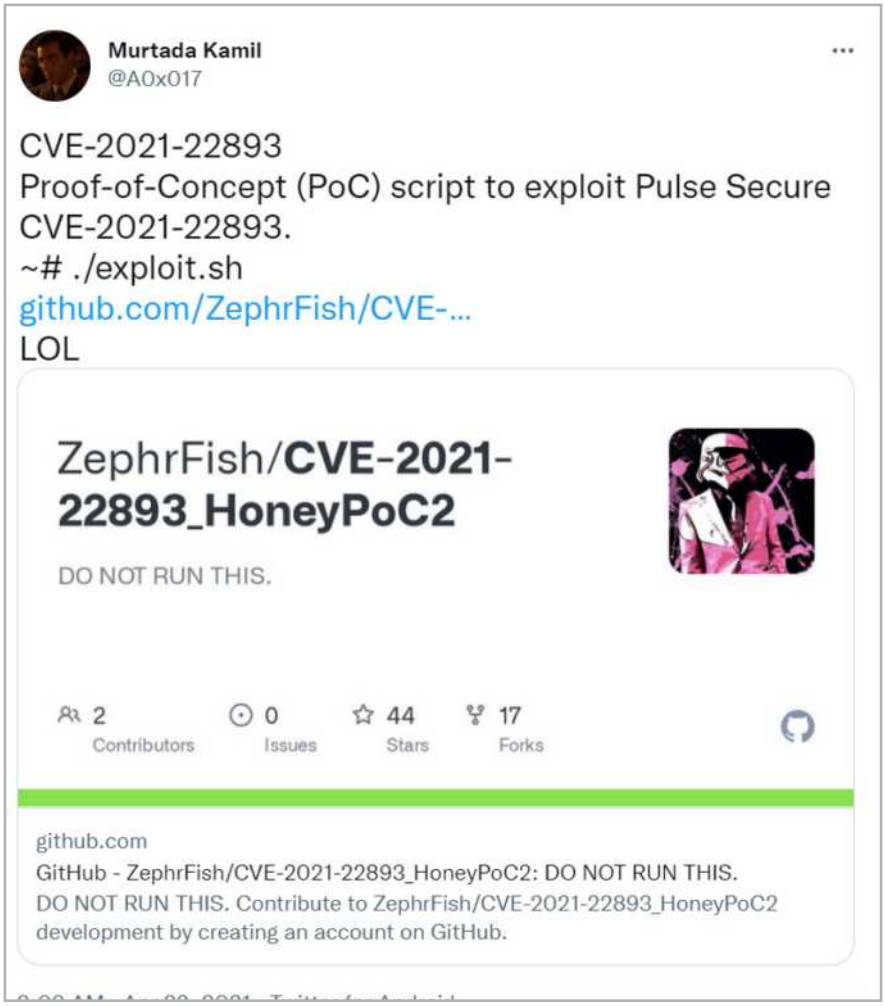
On 20 Apr 2021, Pulse Secure released an out-of-cycle security advisory to alert users of its VPN framework about critical authentication bypass vulnerabilities. The flaw could enable remote, unauthenticated attackers to execute arbitrary code with no user interaction. The relevant set of vulnerabilities tracked in the advisory carried a whopping CVSSv3 base score of 10.

Once again, at the time of disclosure, Pulse Secure did not provide a working patch. What it did provide was a temporary workaround in the form of an XML file that disabled the VPN appliance's Windows File Share Browser and Pulse Secure Collaboration features. It also threw in a tool to support security teams in checking the integrity of the file system and identifying additional or modified files.

That same day, cyber-security firm Mandiant disclosed it had been tracking 12 discrete malware families that were associated with the exploitation of the four vulnerabilities. Although observed in separate investigations, all of the malware types were probably developed by state-sponsored groups. In fact, those four flaws were reportedly used to compromise US and European government, defense, and financial organizations' networks for espionage.

Just three days after the vulnerability disclosure, and with the patch still a couple of weeks away, the first PoCs started to pop up online. Digital Shadows identified the publication of the first largely working patch on 23 Apr 2021, on GitHub. Although we can't say for sure that the PoCs helped other threat groups exploit the flaws, it probably pushed more cybercriminals to test vulnerabilities in Pulse Secure. Pulse Secure finally released a patch on 03 May 2021.

PULSE SECURE	
CVEs	CVE-2021-22893 CVE-2021-22894 CVE-2021-22899 CVE-2021-22900
Zero-Day	Yes
Threat Actors	UNC2630 (APT) UNC2717 (APT)



2.3.3 SUPPLY-CHAIN COMPROMISE

On 23 Dec 2020, American tech company Accellion informed its customers that its decades-old FTA (File Transfer Appliance) application was the target of a sophisticated cyber attack, and that all known exploited flaws had been patched. The damage had already been done, which came to light in February 2021: Cybercriminals had managed to access FTA servers and deploy the web-shell "DEWMODE" in a supply-chain attack. They stole Accellion customers' Structured Query Language (SQL) database hosted on FTA servers.

The attack was unusually attributed to two financially motivated threat groups, "FIN11" and the "Clop" ransomware gang. Supply-chain attacks are typically associated with state-sponsored groups because they require great technical sophistication, but these profit-seeking Accellion attackers were highly skilled in their own right: identifying, exploiting, and chaining four zero-days. CLOP didn't encrypt its victims when dropping ransomware, but exfiltrated sensitive data and emailed the affected companies, threatening to expose their information online unless a ransom was paid.

This event points to a huge red flag: the dangers of zero-days present in third-party vendors, which can open up unauthorized access to multiple organizations. 🚩 Accellion also learned a harsh lesson about applications nearing their end of life: it's still important to keep code secure until they're retired or deprecated.

ACCELLION FTA	
CVEs	CVE-2021-27101 CVE-2021-27102 CVE-2021-27103 CVE-2021-27104
Zero-Day	Yes
Threat Actors	Clop (Ransomware)

THIS INCIDENT HIGHLIGHTS THE DANGERS OF ZERO-DAY VULNERABILITIES WITHIN THIRD-PARTY VENDORS, WHICH COULD LEAD TO UNAUTHORIZED ACCESS BY CYBERCRIMINALS.

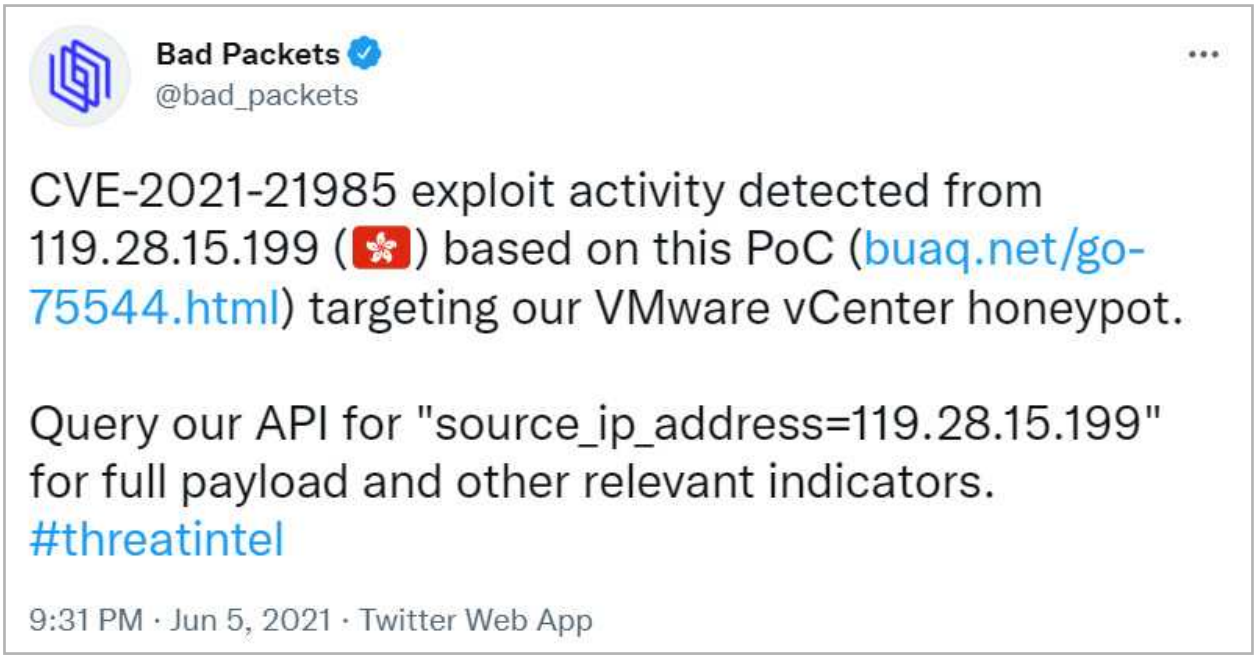
2.3.4 POCS AND MASS SCANNING

VMWARE	
CVEs	CVE-2021-21985
Zero-Day	No
Threat Actors	Darkside (Ransomware) RansomExx (Ransomware)

On 25 May 2021 the American cloud computing company VMware published a security advisory with details of CVE-2021-21985, a critical RCE flaw in its vSphere Client via the Virtual SAN (vSAN) Health Check plug-in (which is enabled by default). To successfully exploit the vulnerability, which carries a CVSSv3 base score of 9.8, an attacker needs network access over Port 443 to execute commands with unrestricted privileges.

In this case, VMware also provided its customers with a patch, but it wasn't the easiest or quickest option for busy or understaffed security teams. As CISA put it, "unpatched systems remain an attractive target and attackers can exploit this vulnerability to take control of an unpatched system". Still, there was hope: "attractive" doesn't necessarily mean exploitable, right? Threat actors would need *certain knowledge* for success here. You can probably guess the ending to this story. A security researcher published a fully working PoC for the flaw on 05 Jun 2021, honeypots began detecting mass scanning for it, and—just like that—active exploitation of the PoC occurred in the wild, with groups such as DarkSide and RansomExx dropping ransomware into targeted environments.

The immediate correlation between the publication of a legitimate PoC and the consequent mass scanning by malicious actors is a powerful reminder of the dual use of PoCs. If you want to guarantee your organization has enough time to patch its system and avoid harmful events, you'd better believe that responsible code disclosure is crucial.



Mass scanning detected on CVE-2021-21985 through legitimate PoC (Source: Twitter)

2.3.5 UNPATCHED LEGACY SECURITY FLAWS

On 02 Apr 2021, the FBI and CISA issued a joint cybersecurity advisory alerting organizations about APT groups gaining initial network access via legacy flaws in a Fortinet VPN product. At the time, several APT groups were scanning and mapping publicly accessible devices over Ports 4443, 8443, and 10443.

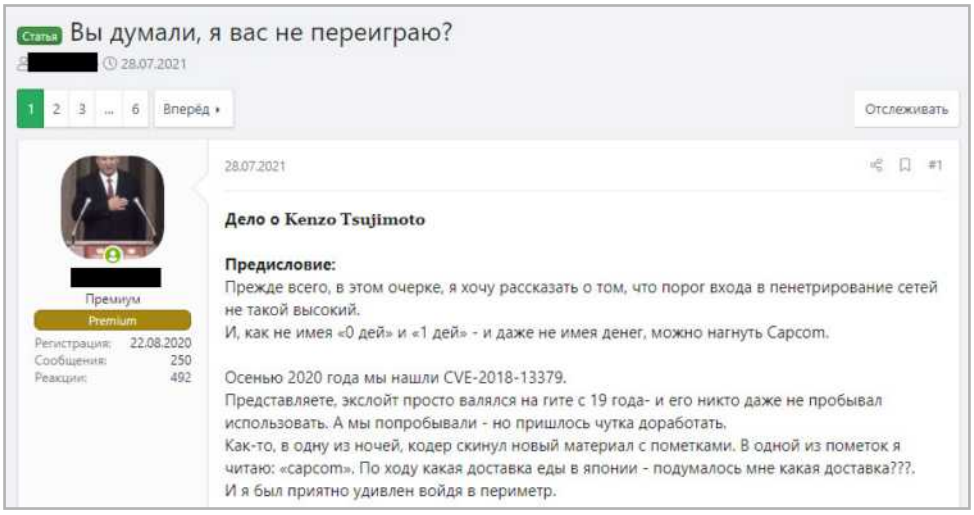
CVE-2018-13379 is a patch traversal flaw in Fortinet's FortiGate SSL VPN that allows a remote, unauthenticated attacker to read arbitrary files via a specifically crafted request. The FBI and CISA have observed this vulnerability chained with other Fortinet flaws to conduct a variety of attacks from cybercriminals and sophisticated state-sponsored groups alike.

The observed APT groups were likely trying to infiltrate multiple organizations in the public and private sectors, to enable future cyber attacks. As the CISA advisory stated, these groups traditionally exploit critical vulnerabilities for "denial-of-service (DoS) attacks, ransomware attacks, structured query language (SQL) injection attacks, spearphishing campaigns, website defacements, and disinformation campaigns".

Exploiting older vulnerabilities goes over big with cybercriminals and threat groups. For the rest of us, we're dealt a powerful reminder of the struggles that security teams face in shaping and maintaining VM programs. In investigating Russian-language cybercriminal forums, we found that of the three CVEs listed by CISA, CVE-2018-13379 was the most discussed; older, unpatched vulnerabilities are an especially tempting fruit. In this instance, highly sophisticated threat groups targeted a three-year old bug—these groups are nothing if not persistent.

FORTINET VPN	
CVEs	CVE-2018-13379 CVE-2020-12812 CVE-2019-5591
Zero-Day	No
Threat Actors	State-sponsored groups Cring (Ransomware)

We also found a post on Exploit by a threat actor discussing how they'd exploited CVE-2018-13379. They said that an exploit for the flaw had been "laying around on Github since 2019" 🚩 and that "no one even tried to use it". Upon testing it out, the enterprising cybercriminal found themself "pleasantly surprised". As if this image isn't disturbing enough, our intrepid Exploit user said they went on to benevolently share their research with the "Conti" and "Nefilim" ransomware groups. But we can't blame this single individual. In their own words: "All the methods described by me are on Google - on the official product sites."...everything they needed for exploitation was right there in open sources, unearthed with a little light excavation.



Exploit user detailing exploitation of CVE-2018-13379

3. WORD ON THE STREET: WHAT ARE CYBERCRIMINALS SAYING ABOUT EXPLOITS?

The Photon Research Team gathered extensive primary and secondary data for this paper, and blue teams all over the world are doing the same thing, every day, to keep up with the vulnerability threat landscape. But other actors are lurking behind the scenes: Cybercriminals and state-sponsored groups constantly scan the Internet for precious resources to stay ahead of the curve and beat security defenders on the clock.

In addition to our monitoring of the cybercriminal community to stay abreast of crucial topics (ransomware trends, Initial Access Broker activity, popular TTPs), we keep our finger on the pulse of vulnerability threats and have staggering results to share with you. This scene 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.

We've observed some key trends in the dialogue on cybercriminal forums over the past years. And we've identified key types of threat actors active on these platforms. Allow us to introduce you to this lively community; as a security defender, you're not welcome in their space, but you can learn a lot from peering through the curtains.

SO DON'T BE SURPRISED WHEN WE TELL YOU THAT CYBERCRIMINALS AND STATE-SPONSORED GROUPS ARE CONSTANTLY SCANNING THE INTERNET FOR PRECIOUS RESOURCES TO STAY AHEAD OF THE CURVE AND BEAT SECURITY DEFENDERS ON THE CLOCK.

3.1 HOT RIGHT NOW: EXPLOITATION TRENDS

3.1.1 HIGH-STAKES SALES AND EXPLOIT-AS-A-SERVICE

Let's start at the top of the cybercriminal pyramid. The market for zero-days is an extremely expensive and competitive one, and it's usually been a prerogative of state-sponsored threat groups. However, as we've frequently discussed over the past years, certain high-profile cybercriminal groups (read: ransomware gangs) have amassed incredible fortunes and can 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 during our investigations. These prices can appear enormous but there's a key aspect to keep in mind. Whatever legitimate bug bounty programs offer (and we've often seen them offering multi-million dollar bounties before), 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. 🚩

But for those who feel like they're missing out on all the zero-day fun, there's another option (the cybercrime community doesn't leave anyone behind). During our investigation, we've observed cybercriminals discussing the potentialities of an "exploit-as-a-service" model for the first time. This model would allow capable threat actors to "lease" zero-day exploits to other cybercriminals to conduct cyberattacks. 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 enables zero-day developers to generate substantial earnings by renting the zero-day out while waiting for a definitive buyer. Additionally, with this model, renting parties could test the proposed zero-day and later decide whether to purchase the exploit on an exclusive or non-exclusive basis.

We don't know how long this model will remain viable. 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.

3.1.2 OLD-BUT-GOLD VULNERABILITIES

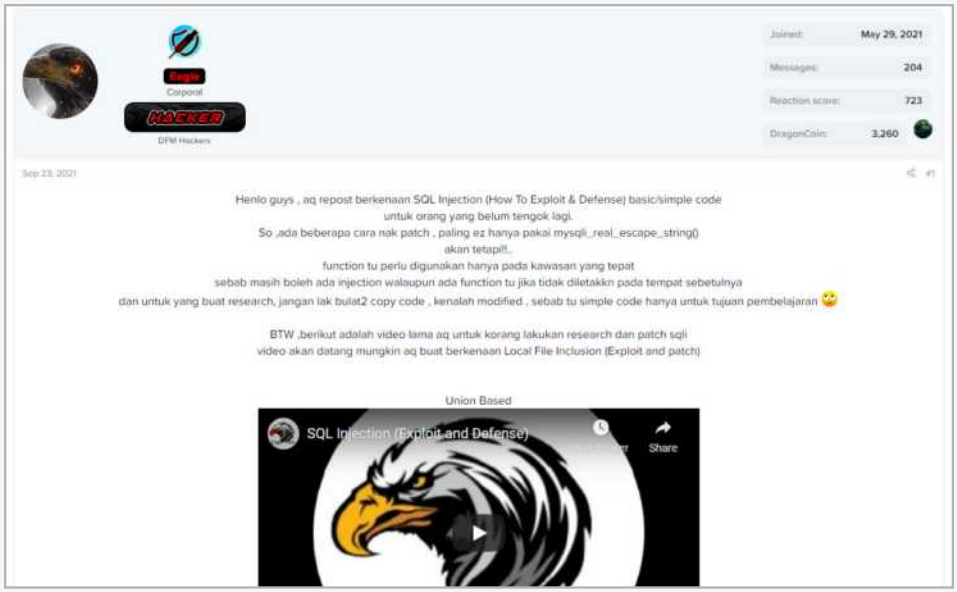
New zero-day vulnerabilities signify fresh and undiscovered issues, ripe for exploiting when we're none the wiser. Ambitious and technically competent threat actors are constantly rushing to snap up the shiniest security flaw out there. But older, already disclosed vulnerabilities can also help cybercriminals strike gold; they depend on the certainty that some organizations out there still haven't gotten around to updating that product they forgot they have, or that technology they assumed was free of flaws. If you need proof: We've seen threat actors share a whole database of companies yet to apply patches for the Microsoft Exchange Server vulnerabilities mentioned above.

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.

EXISTING VULNERABILITIES CAN HELP CYBERCRIMINALS STRIKE GOLD, AND THEY CONTINUE TO CAPITALIZE ON THE FACT THAT THERE STILL WILL BE SOME ORGANIZATIONS OUT THERE THAT HAVE YET TO UPDATE THE PRODUCTS AND TECHNOLOGIES THEY USE.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
ip	full	port	Domains	Product	Hostnames	ISP	Server	Common Na	Organizat	Cou	Country	City	Vulns	ZI Company	ZI Headquar	ZI Revenue	loyees	ZI Website	ZI Industries	ZI Link	emails	phones
213.181.118.20	yes	443	["hve.is"]	Microsoft IIS	["postur.hve.is	Nova hf	Microsoft-IIS/8.5	*.hve.is	Hellbrigðis	IS	Iceland	Reykja	["CVE-2021-34473	Nova	Lágmúli 9, Re	$15 Million	75	www.nova.is	Telephony &	https://www.z	gunnar@nov	+354 519 100
212.30.252.87	yes	443	["skrin.is"]	Microsoft IIS	["87.252.ptr.sk	Advania Isla	Microsoft-IIS/8.5	postur.stapi.is		IS	Iceland	Akurey	["CVE-2021-34473	Hringdu	Grensasvegi	$5 Million	25	www.hringdu.is	Telephony &	https://www.zoominfo.com/c		+354 537 700
200.46.135.88	yes	443	[]	Microsoft IIS	[]	Cable Onda	Microsoft-IIS/10.0	movil.etesa.com.pa		PA	Panama	Coclé	["CVE-2021-34473	Etesa	Plz Sun Towe	$7 Million	30	www.etesa.com.pa	Electricity, Oi	https://www.zoominfo.com/c/etesa/425367		
200.46.238.114	yes	443	["fpbbank.co	Microsoft IIS	["Smtp2.fpbba	Cable Onda	Microsoft-IIS/8.0	webmail.fpbb	FPB Bank	PA	Panama	Colón	["CVE-2021-34473	FPB Bank		$6 Million	30	www.fpbbank.com	Banking, Fina	https://www.zoominfo.com/c/fpb-bank-inc/		
190.61.82.140	yes	443	["ingenieriarm	Microsoft IIS	["mail.ingenier	UFINET PA	Microsoft-IIS/8.5	mail.ingenieriarm.com		PA	Panama	Panamá	["CVE-2021-34473	Ingeniería R	San Francisc	$5 Million	<25	www.ingenieriarm.	Architecture,	https://www.zoominfo.com/c/ingenieria-r-m		
190.205.61.117	yes	443	["universalde	Microsoft IIS	["mail2.univer	CANTV Ser	Microsoft-IIS/8.0	univserver		VE	Venezuela	Caracas	["CVE-2021-34473	Universal de	Ave Avila c/ Av	$89 Million	356	www.universaldes	Insurance	https://www.z	anabelg@segurosca.com	
190.205.124.13	yes	443	["cantv.net"]	Microsoft IIS	["190-205-124	CANTV Ser	Microsoft-IIS/10.0	Correo.Resto	Restoven	VE	Venezuela	Caracas	["CVE-2021-34473	Restoven de	El Recreo, C	$500 Million	2560	restoven.com	Restaurants,	https://www.zoominfo.com/c/restoven-de-ve		
200.46.33.136	yes	443	["gjp.com.pa"	Microsoft IIS	["mail.gjp.com	Cable Onda	Microsoft-IIS/8.5	mail.grupolospueblos.com		PA	Panama	Panamá	["CVE-2021-34473	Grupo Los Pueblos		$8 Million	36	www.gjp.com.pa	Real Estate	https://www.z	cads@grupolospueblos.com	
201.218.247.90	yes	443	["capitalbank	Microsoft IIS	["mail.capitalb	Cable Onda	Microsoft-IIS/8.5	mail.capitalbank.com.pa		PA	Panama	Panamá	["CVE-2021-34473	Capital Bank	P H Global Pl	$27 Million	136	www.capitalbank.c	Banking, Fina	https://www.zoominfo.com/c/capital-bank-in		
200.46.253.34	yes	443	["talal.com"]	Microsoft IIS	["correo.talal.c	Cable Onda	Microsoft-IIS/8.5	correo.talal.c	TALAL	PA	Panama	Colón	["CVE-2021-34473	Tapia , Linare	Paseo Rober	<$5 Million	<25	www.talal.com	Law Firms & Legal Services	alinares@talal.com		
45.225.70.14	yes	443	[]	Microsoft IIS	[]	Trans Ocea	Microsoft-IIS/7.5	mail2.atlasbank.com		PA	Panama	Panamá	["CVE-2021-34473	Atlas Bank	689 5th Ave,	$5 Million	<25	www.atlasbank.co	Banking, Fina	https://www.zoominfo.com/c/atlas-bank-sa		
186.5.136.187	yes	443	[]		[]	Columbus N	nginx	*.migracion.gob.pa		PA	Panama	Panamá	["CVE-2021-34473	Direccion Na	Panama	$50 Million	266	www.migracion.go	Public Safety	https://www.zoominfo.com/c/direccion-nacio		
186.74.177.164	yes	443	[]	Microsoft IIS	[]	Cable & Wir	Microsoft-IIS/8.5	owa.sc.sunin	Sun Intern	PA	Panama	Panamá	["CVE-2021-34473	Sun Internati	209 Aramist A	$1 Billion	14632	www.suninternatio	Lodging & Re	https://www.zoominfo.com/c/sun-internationa		
201.218.210.10	yes	443	[]	Microsoft IIS	httpd	TECNOLO	Microsoft-IIS/10.0	ptyvexch01		PA	Panama	Panamá	City	Tecnasa U	Calle Ruben	$30 Million	159	www.tecnasa.com	Software & Te	https://www.z	gabyaued@gmail.com	
168.77.213.71	yes	443	["senadis.go	Microsoft IIS	["mail.senadis	Autoridad N	Microsoft-IIS/10.0	mail.senadis.gob.pa		PA	Panama	Panamá	["CVE-2021-34473	TopManage	Ave Ricardo J	$18 Million	95	www.topmanage.c	Engineering &	https://www.zoominfo.com/c	+507 300-720	
200.35.109.12	yes	443	["avior.com.ve	Microsoft IIS	["mail.avior.co	TELEFONIC	Microsoft-IIS/8.5	*.avior.com.ve		VE	Venezuela	Barcelo	["CVE-2021-34473	Avior Airlines	Aeropuerto In	$170 Million	825	www.avior.com.ve	Airlines, Airpo	https://www.z	ramirez_luis	+58 501-2846

Shared database of negligent MS Exchange Server users, as shared on cybercriminal forum XSS



Video tutorials taking users through different ways to conduct SQL injection

3.1.3 KNOWLEDGE IS POWER, SHARING IS CARING

Just as the intelligence community thrives on information sharing, cybercriminals exchange knowledge. When it comes to vulnerabilities, there is a slew of information being slung about on underground cybercriminal platforms. To overcome exploitation challenges, they often tap on each other's knowledge and crowdsource information or initiate a thread; those who already are proficient can choose to impart some of their wisdom.

Besides sharing tutorials, experienced, trusted users often provide reviews of their preferred (or least favorite) tool on the market, just like any other good consumer would. Reviews cover everything from vulnerability-scanning tools to online bulletproof-hosting services,[4] and many include detailed descriptions of how they work. These diligent reviewers are helping their peers identify relevant products for exploitation and make more informed decisions.

Alongside these well-meaning cybercriminals helping novices, there are other cybercriminals attempting to scam or troll forum members. At the end of the day, criminals will be criminals. But we've also noticed experienced forum members warning newer users—another form of generosity that improves threat actors' ability, and causes more sleepless nights for security managers.

User of Chinese-language forum recommending a tool and offering self-developed ones

[4] A bulletproof host is an illegitimate service that allows customers to conduct any kind of malicious activity with protection against law enforcement.

OPSEC: A FORCE FOR GOOD...AND BAD

Broadly, operation security (OPSEC) refers to measures to prevent sensitive information from reaching an unintended audience, such as potential adversaries. Intelligence practitioners often use OPSEC for confidential information pertaining to targets—information that should only be shared with vetted parties.

Cybercriminals also practice some form of OPSEC. Many are aware that law-enforcement officials lurk on the same sites they're active on, so they take measures to ascertain the legitimacy of users they communicate with. Although many discussions and transactions occur on underground cybercriminal platforms, no one is likely to give away information overtly and freely without conducting some verification.

User of Exploit forum advertising a service to identify companies with exposed vulnerabilities

3.2 WHO'S WHO: MEET THE CONTRIBUTORS EXPLOITING OUR VULNERABLE WORLD

The cybercrime underground harbors a diverse set of actors, and every one contributes to the scene. We've mentioned a handful throughout this piece, and we'll categorize them here (acknowledging there can be major crossover). Who are these enterprising members of the exploitation community?

- **High-rollers: We've already mentioned the threat actors selling and buying zero-day exploits for $1,000,000-plus...big wallets, possibly bankrolled by a nation-state, sometimes just successful entrepreneurs.**
- **General merchants: Other sellers deal in less-critical vulnerabilities, exploit kits, and databases listing the names and IP addresses of companies that have unpatched vulnerabilities.** 🚩
- **General buyers: Interested buyers are "techie", as a bare minimum (and wealthy in rare cases...see first bullet). These actors often wait for exploit prices to lower before buying from other cybercriminals.**
- **Code communicators: The threat actors who share and advertise PoCs on GitHub have an enduring role on forums—newly discovered vulnerabilities create a demand for PoCs—and the cycle repeats itself indefinitely.**
- **Show-offs: Not surprisingly, some members of the vulnerability community can't help but showcase their technical expertise. It's very common to see them discuss vulnerabilities in incredible depth, or enter forum competitions, or freely share knowledge on how to perform an exploit. And they have an audience that needs to be fed...**
- **Newbies: Less-technically inclined users absorb information from their experienced peers and apply it; they might even recycle it on various platforms. Their intentions for sharing this information may be based on "good faith", or they may just be looking to inflate their reputation for sharing "original" information.**
- **Newshounds: Finally, there are community contributors who regularly share articles and fresh news related to recently disclosed vulnerabilities. On the Russian-language forums XSS and Exploit, it's quite common for a user to share media reports on vulnerabilities and translate them from English to Russian, or vice-versa.**

4. MITIGATE, REMEDIATE: BUILD A FORTRESS AROUND YOUR FRAMEWORK

4.1 A RISK-BASED APPROACH

The IT landscape of 2021 is a highly complex fusion of emerging technology and legacy infrastructure. The latter comprises formerly traditional IT assets; the former comprises mobile devices, apps, cloud infrastructure, containers, Internet of Things (IoT) devices, and operational technology assets. The relationships among these differing forms of technology can often impede visibility of security risks. Workarounds or stopgaps are being used while security teams scramble to find solutions in an ever-increasingly complicated architecture.

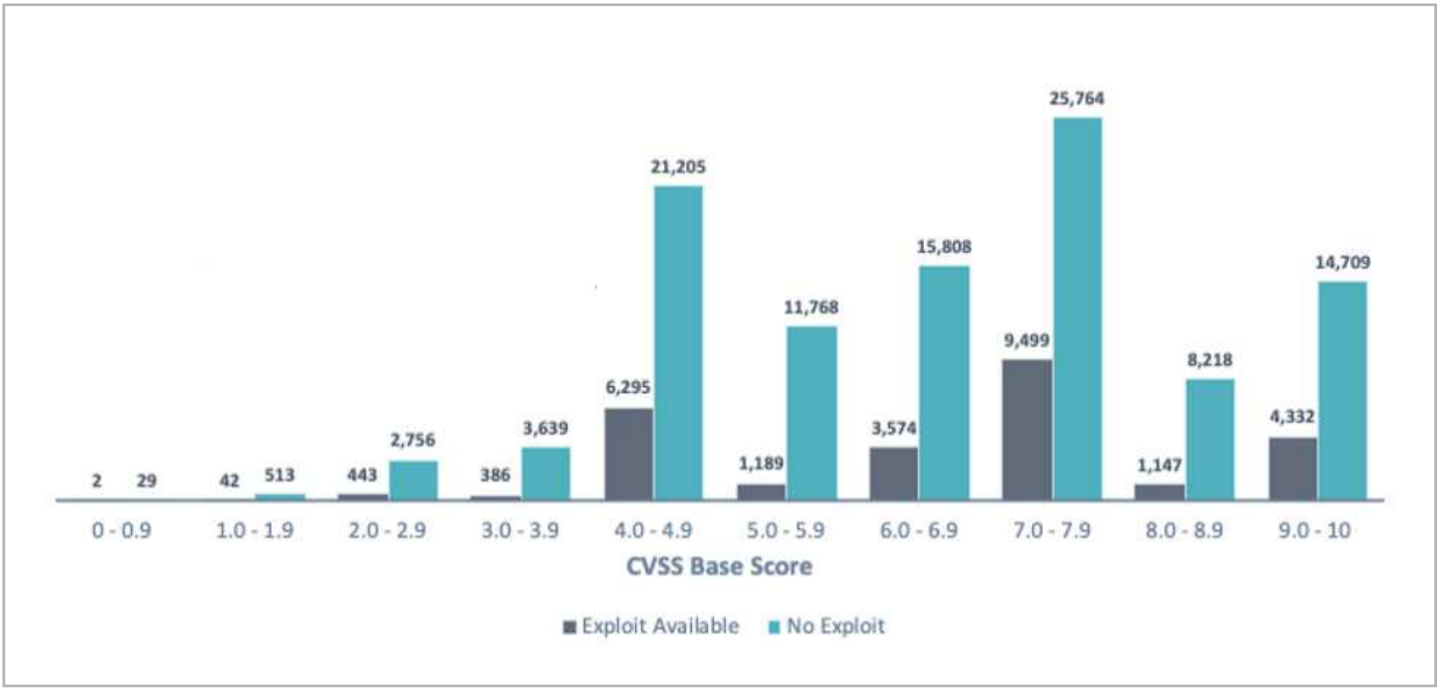
Security defenders are further confounded by traditional VM processes failing to incorporate threat intelligence and triage assets based on a calculated risk. Ultimately, this leaves a difficult task: too many vulnerabilities with too little time to patch effectively.

A risk-based vulnerability management (RBVM) process reduces vulnerabilities across your organization by prioritizing remediation and basing it on immediate risks. Additionally, it offers context for the potential business risk those bugs bring. With this approach, you:

1. **Gain visibility of all assets**
2. **Scan and monitor for a broad range of attack methods**
3. **Judge, for each asset:**
    - **Its value**
    - **How critical it is to business continuity**
    - **How vulnerable it is**
4. **Identify existing controls and current threat intelligence**
5. **Prioritize results based on the above context**

RBVM is the most efficient way to shrink the potential attack surface. Ultimately, it bolsters your overall cyber-resilience.[5] We'll go over the above steps in more detail. But first, a word about CVSS scores.

[5] An organization's ability to prepare for, respond to, and recover from cyber attacks and security breaches



Exploit availability per CVSS base score (Source: Tenable)

4.1.1 THE LIMITED USEFULNESS OF CVSS

When triaging risks, many companies still rely on the CVSS scores assigned to vulnerabilities. But those scores are only aimed at providing an understanding of the technical severity of a particular vulnerability. CVSS doesn't reflect its exploitability, or how widespread its impact may be felt. It doesn't represent up-to-date threat intelligence that would reveal its use in current threat campaigns. And it doesn't take into consideration whether compensating controls are already in place, nor how important the affected asset is. (A medium vulnerability in a critical asset should always be remediated before a critical vulnerability on a non-important system.)

CVSS does not incorporate these factors to help you determine risk, but you should. And bear in mind, also, that only a fraction of the enormous pool of high and critical vulnerabilities are ever exploited in the wild; some vulnerabilities with lower severity scores are just as likely to be exploited in live attacks. CVSS should not be used as the arbiter of whether a vulnerability should be remediated or not; instead, focus on the overall risk each bug poses, with the exploitability of the vulnerability being a key factor.

ULTIMATELY, USING A RISK-BASED APPROACH SUPPORTS SECURITY TEAMS IN OVERCOMING SOME DAY-TO-DAY CHALLENGES WE'VE MENTIONED THROUGHOUT THIS PAPER.

4.1.2 REGISTERING AND PRIORITIZING ASSETS

An RBVM process starts with a comprehensive review of every identifiable asset on a network. As highlighted earlier, unidentified and unpatched assets present a significant risk. Asset registers need to incorporate traditional IT, like servers and endpoints, in addition to cloud-based assets, mobile phones, and IoT devices. They should continually be managed and adjusted as assets are added or become obsolete and are decommissioned. With all assets identified, the overall attack surface comes into sharper focus.

The next step is categorizing the assets by operational priority, identifying each asset's business-specific purpose. Assign each asset a priority level or number based on business importance, threat context and the vulnerability's severity. At this stage, executive approval is required to ascertain the organization's "risk appetite"—how much risk it's willing to swallow while pursuing its objectives—before any risk-reducing action is deemed necessary.

Now any assets designated a business risk can be added to your organization's VM platform. Most modern platforms have a range of functionality, which should include:

- **Automatic connection and detection of all network-connected assets**
- **Incorporation of the business value assigned to each asset**
- **Insights from a range of threat intelligence feeds, to provide context, about CVEs**
- **Options for in-depth reporting and filtering of results**
- **Prediction of likelihood that a CVE will be exploited, via Machine Learning modelling**
- **Production of accurate, risk-based analytical scores for all vulnerabilities, weighted by the organization's risk appetite and likelihood of exploitation**

MORE ISN'T ALWAYS A SYNONYM FOR BETTER - AND THIS IS CERTAINLY TRUE WHEN IT COMES TO INTELLIGENCE.

4.1.3 TREATING AND REPORTING VULNERABILITIES

It's time to take action on the identified vulnerabilities. This can go one of three directions: remediate/fix the vulnerability, mitigate/lessen the likelihood of an exploitation by using compensating controls (often the best option when a patch isn't available or thoroughly tested), or acceptance with no action taken. Action should depend enormously on the type of vulnerability, risk appetite, and resources available.

Once action has been taken, regular and continuous reporting will aid VM efficiency. Not only does this kind of reporting help IT teams easily understand which remediation techniques will help them fix the most vulnerabilities with the least amount of effort, it helps security teams monitor vulnerability trends over time in various parts of their network, and it helps support the organization's compliance and regulatory requirements. And the real bonus is a drop in your overall cyber risk, over time.

Aiming to patch everything, here, now is practically impossible for most blue teams out there. On the other hand, learning to effectively prioritize is a crucial skill in this field and will ultimately be the hallmark of your VM program's effectiveness.

4.2 VULNERABILITY INTELLIGENCE

Although rewarding, effective risk-based prioritization with VM can be an energy-consuming process. Along with the many human and financial resources it takes for implementation, every security team needs plentiful high-quality intelligence to make informed decisions that have real-world implications.

How much intelligence does your security team need? "More" is not always a synonym for "better"—certainly not when it comes to intelligence. Tailor your intelligence needs to your threat model, such as with a representation of the potential threats to your organization from a hypothetical attacker's point of view. In practice, this means adjusting your intelligence requirements to your needs.

Incorporating vulnerability intelligence will help you prevent and quickly mitigate the most relevant threats for your specific organization. Be aware that gathering and processing massive amounts of information into precise, timely, relevant intelligence requires human skills that are hardly scalable in the classical business-y way. Sometimes in-house resources are devoted to this end, and sometimes the work is outsourced. Either way, the intelligence will help prioritize patching schedules based on: active threats to your sector and location, the presence (or absence) of a working PoC code in the wild, and the use of affected software or hardware by your organization or by a third party.

Once fused into your organization's threat model, vulnerability intelligence can be used across a variety of internal functions to improve security planning. In particular, it can support the following.

1. **Triaging:**
   Vulnerability intelligence can help you spot key security flaws that may affect your organization in a sea of security flaws. New vulnerabilities are disclosed at an unprecedented rate and most of them will not be relevant to your organization (despite what security headlines say). Then again, neglect to patch certain flaws and you could invite devastating results. Instead, take our advice: study, prioritize, triage. In that order.

2. **Communicating:**
   VVulnerability intelligence can also support you when dealing with key executives in your organization. Being able to effectively communicate risks and opportunities across your company is a crucial skill, and one that takes time to develop. By presenting vulnerabilities as part of a broader context—not merely as CVE numbers—you can effectively convey real risk and probability, helping you win managerial approval to patch appropriately. You can now make them finally see that the "if it ain't broke, don't fix it" approach is no longer sustainable.

3. **Mitigating:**
   Patching your vulnerable hardware and software isn't the end of the story. Some of you will already know that the intelligence process is typically represented as a cycle, with every action informing the next one. As such, every patching round will inevitably inform the next one and will result in an adjusted security plan based on empirical evidence.

Patching your vulnerable hardware and software isn't the end of the story. Some of you will already know that the intelligence process is typically represented as a cycle, with every action informing the next one. As such, every patching round will inevitably inform the next one and will result in an adjusted security plan based on empirical evidence.

About Digital Shadows

Digital Shadows minimizes digital risk by identifying unwanted exposure and protecting against external threat. Organizations can suffer regulatory fines, loss of intellectual property, and reputational damage when digital risk is left unmanaged. Digital Shadows SearchLight™ helps you minimize these risks by detecting data loss, securing your online brand, and reducing your attack surface.

To learn more and get free access to SearchLight™, visit
www.digitalshadows.com

London, UK **San Francisco, CA** **Dallas, TX**

Authors: Digital Shadows Photon Research Team

digital shadows_