SKYBOX SECURITY

Vulnerability and Threat Trends Mid-Year Report 2021

Critical infrastructure risk emerges as top concern

Contents

Introduction

Gidi Cohen, CEO and founder, Skybox Security

Cybercrime thrives in times of instability, and it's hard to think of a more disruptive period for enterprises than the past year and a half. The COVID-19 pandemic and the on-again-off-again reopening have spurred the kind of breakneck technological changes that create abundant new openings for malicious actors and a host of new challenges for CISOs and their teams.

We're seeing the effects play out in the first half of 2021. This report reveals a threat landscape that's expanding and diversifying at a dizzying rate. Vulnerabilities are increasing precipitously and inexorably, particularly in sensitive areas such as operational technology (OT) and network devices, putting vital infrastructure at risk.

As new vulnerabilities arise, attack vectors are springing up to exploit them and capitalize on emerging economic opportunities. Witness the boom in cryptomining malware and the ongoing growth of ransomware. Threat actors now have a robust set of tools and a flourishing ecosystem to support their endeavors. Vendors of exploit kits and malware-as-a-service make it simpler than ever to mount campaigns and launch attacks, with cryptocurrency easing the movement of money and collection of ransoms.

The frequency and scope of malicious activity are increasing apace. Exploits in the wild are on the upswing, as this report details, and so far 2021 has seen some of the most audacious and potentially devastating cyberattacks in history—some exploiting OT and network vulnerabilities to disrupt vital facilities such as public utilities and energy infrastructure.

At the same time, security organizations have had their hands full managing the massive technological shifts required by the pandemic, while also coping with staffing limitations and a slew of competing priorities.

The writing is on the wall: the traditional, scattershot approach to vulnerability management, which overlooks many actual risks while overstating others, is a losing strategy in an era of exploding threats and security teams that have to do more with less. Enterprises need precise, exposure-based solutions that cut through the noise, pinpoint the real security threats and enable practical, cost-effective remediations.

Key findings

Unless otherwise noted, all of the statistics in this report come from Skybox Research Lab and cover the first six months (H1) of 2021. See the Methodology section for more details.

Vulnerabilities continue to climb.

There were 9,444 new vulnerabilities reported in H1 2021, not far off last year's record-setting pace. These new vulnerabilities add to a daunting cumulative total that's making it harder than ever for security organizations to make a dent without knowing which vulnerabilities present the highest risk.

OT vulnerabilities surge, putting critical infrastructure at risk.

New vulnerabilities in OT devices were up 46% versus H1 2020. These vulnerabilities pose a growing threat to critical infrastructure and other vital systems, made manifest in a series of high-profile attacks on facilities such as oil pipelines, water supplies and food processing facilities. To make matters worse, it can be difficult or impossible to identify and remediate OT vulnerabilities through scanning and patching.

Threat actors are taking increasing advantage of vulnerabilities.

More vulnerabilities present more opportunities for exploits, and threat actors are definitely taking advantage. The number of new vulnerabilities exploited in the wild increased 30% relative to the same period last year.

Cryptojacking is the hot new malware trend.

While new malware increased in almost every category, cryptojacking topped the list. This type of malware, which hijacks computer systems for cryptocurrency mining, more than doubled. This is just the latest example of how dynamic an industry malware has become, quickly adapting its offerings and business models to serve emerging markets.

Network infrastructure is increasingly at risk.

Network device vulnerabilities rose by nearly 20% compared to H1 2020. Products such as routers, VPNs (virtual private networks) and firewalls—intended to power and protect networks—are in many cases providing new entry points for malicious actors. As with OT systems, network devices can be difficult to scan and patch.

New vulnerabilities in OT devices

+46%

vs H1 2020

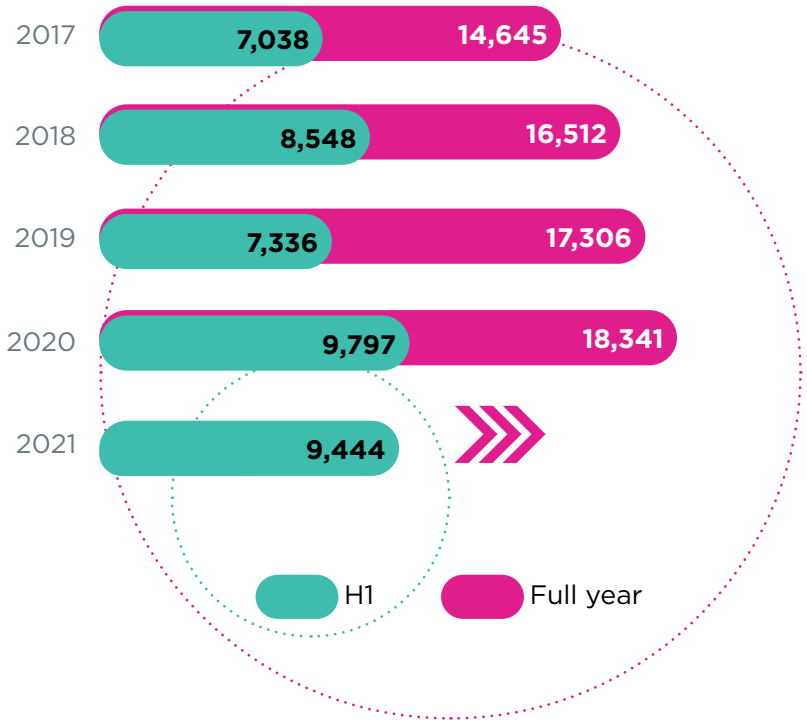
9,444

Total new vulnerabilities reported in H1 2021

Vulnerabilities proliferate

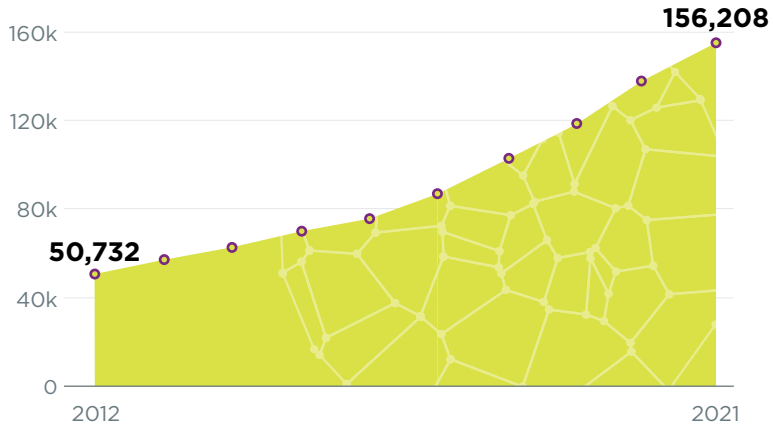
Last year was a record-breaker, and this year is on a similar trajectory. Overall, there were 9,444 vulnerabilities published in the NVD (National Vulnerability Database) in H1 2021, compared to 9,797 published in the same period last year. While there have been some minor up-and-down fluctuations in new vulnerabilities in recent years, the general trend remains steadily upward.

New vulnerabilities over 5 years



It's not just new vulnerabilities that are surging. Most important, the cumulative number of vulnerabilities is increasing relentlessly year after year, more than tripling over the last decade. It's that cumulative number that should concern security professionals the most. The vast majority of vulnerabilities aren't new, and the older they are, the more time hackers have had to find them and exploit them. While security teams rush to respond to the latest advisories, older vulnerabilities may fall off the radar. They can lurk for years in networks, seemingly out of harm's way, only to become exposed later, offering rich targets for attackers. In fact, some of the most exploited vulnerabilities are 4 years old or more.[1]

Vulnerabilities have tripled over the past ten years

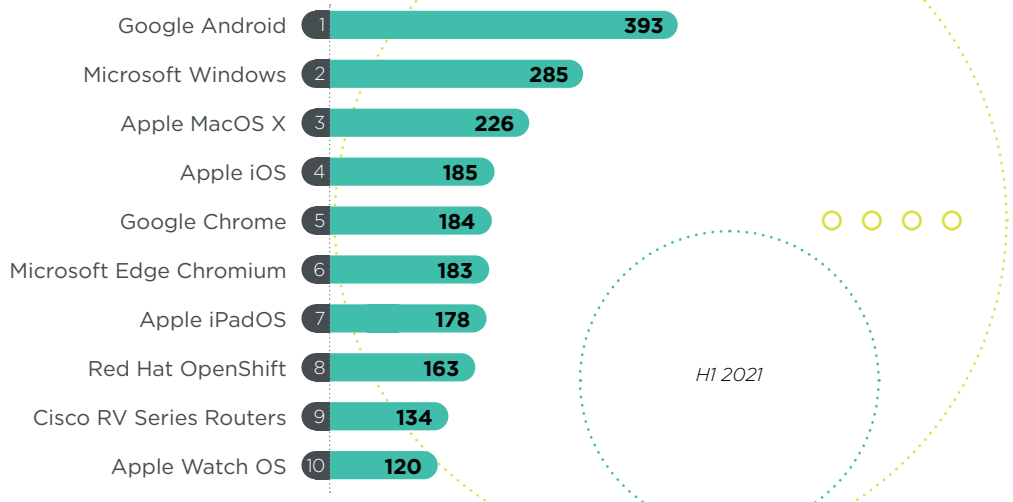


Cumulative vulnerabilities

[1] *This years-old Microsoft Office vulnerability is still popular with hackers, so patch now,* ZDNet, March 16, 2021.

Vulnerabilities aren't just growing in volume; they're spreading across a greater variety of products and device types.

Products with the most new vulnerabilities



The sheer volume and variety of accumulated security debt—hundreds of thousands or even millions of vulnerability instances within some large organizations—means that security teams can't possibly isolate and patch all of them. Nor do they need to. Some vulnerabilities, even those rated as high severity according to the CVSS (Common Vulnerability Scoring System), pose little or no risk because attackers can't get to them. Others, even when rated as low or medium severity, present a clear and present danger because of their accessibility. It's therefore critical to measure actual exposure and identify the greatest, most immediate risks to the organization, regardless of the age or CVSS-based severity of the vulnerabilities.

[2] *Top 10 Routinely Exploited Vulnerabilities,* CISA, May 12, 2020.

SKYBOX SECURITY

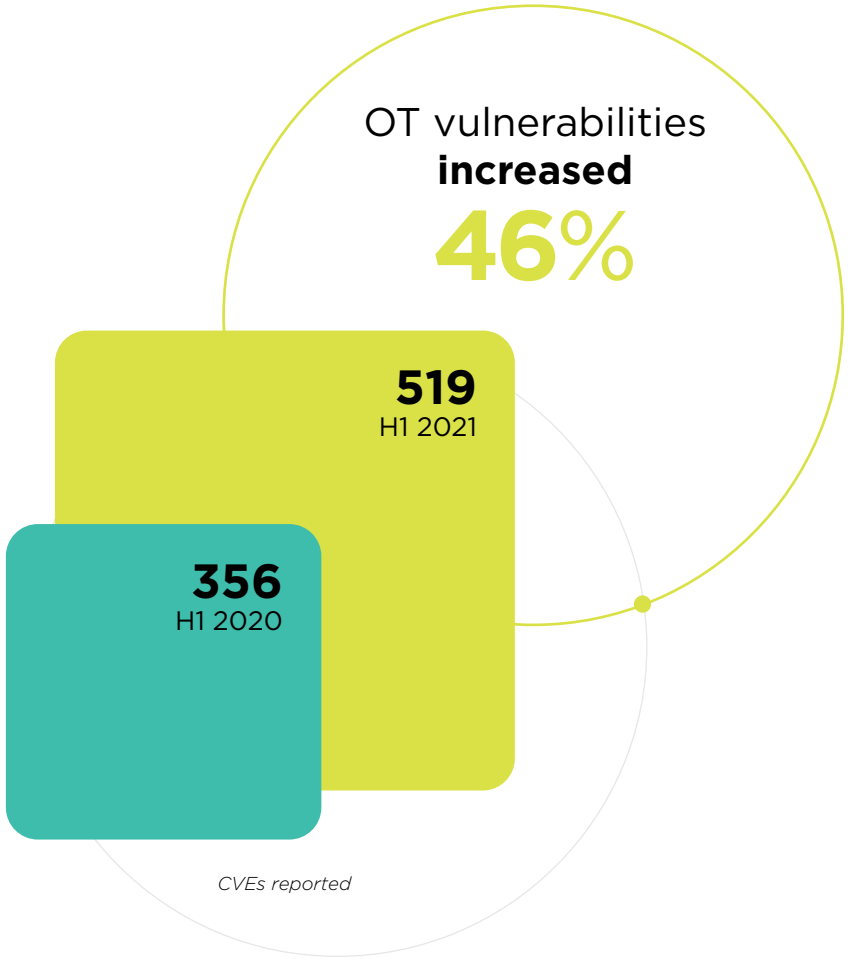
"Cyber actors continue to **exploit** publicly known—and often dated—software vulnerabilities against broad target sets, including public and private sector organizations worldwide."[2]

OT risks jump sharply

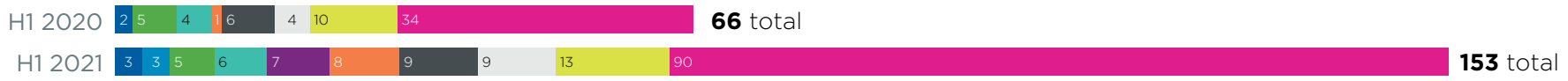
One area that saw a particularly sharp increase in vulnerabilities in H1 2021 is OT, with 519 CVEs (common vulnerabilities and exposures) reported by CISA, compared to 356 CVEs in H1 2020. That's a leap of 46%. CISA advisories on OT vulnerabilities grew similarly, by 45%.

Threat actors are taking advantage of these OT weaknesses in ways that don't just imperil individual companies but also threaten public health and safety and the economy as a whole (see sidebar: "Operational technology under siege").

Nearly all major vendors of OT equipment reported increases in vulnerabilities, especially Siemens. The number of new unique CVEs assigned to Siemens vulnerabilities doubled in H1 2021 versus the same period last year. This could be in part because Siemens is a leader in market share and sells a greater variety of products[3], or perhaps because of more thorough reporting by the company during this period.



CISA advisories by **vendor**



January through June 2021

- Philips
- CODESYS
- General Electric
- Johnson Controls
- Hitachi ABB Power Grids
- Delta Electronics
- Schneider Electric
- Advantech
- Rockwell Automation
- Siemens

[3] *Estimated global factory automation market share in 2019,* by manufacturer, Statista, January 6, 2021.

OT security has become a growing cause for worry in recent years. As Gartner® Research puts it, **"OT systems are usually the crown jewels for organizations. They are core systems for value and revenue creation. If they go down, they cripple operations."**[4] OT is the backbone of energy systems and other basic utilities, communication systems, building automation, physical security systems, vehicle controls and more. Despite the criticality of these facilities, the security measures in place on OT products are often weak or nonexistent. For example, many devices still use generic default passwords and have insecure APIs and protocols that don't enforce proper authentication.

According to Gartner, "Organizations continue to face acute and growing shortages of OT security skills."[5] As companies attempt to drive operational efficiencies by shifting OT management to IT departments or third parties doing remote management, there are fewer hands-on technicians attending to OT devices.

The skyrocketing number of OT devices in many organizations, fueled in part by the explosion of industrial internet-of-things (IIoT) products, is adding to the challenge. Large organizations have thousands of such assets deployed, each with its own security issues. To make matters worse, many of these formerly air-gapped systems are now being connected to networks for purposes of automation and remote monitoring and maintenance, exposing them to external threats.

Hackers are increasingly taking aim at OT systems as low-hanging fruit, and ransomware attacks are becoming commonplace. Cybercriminals know how indispensable OT assets and the systems they control are, and that companies will pay hefty ransoms to avoid disruptions and shutdowns.

While OT vulnerabilities have become a high-value target for threat actors, those same flaws are often invisible to security teams. That's because many OT systems are hard or impossible to scan. At best, companies scan them infrequently (once or twice a year) because they can't afford to take these mission-critical systems offline or degrade service. Likewise, patching many OT systems is technically impossible or too cumbersome and costly to address all vulnerabilities.

As a result, reliance on traditional scan-and-patch methods is a non-starter when it comes to OT security. Security teams can't find the majority of OT vulnerabilities using scanning alone, and even if they could, they wouldn't be able to comprehensively address those flaws using patching. A new approach is needed: one that improves detection and eliminates the blind spots and also facilitates targeted, effective remediation. The latter can be accomplished by evaluating actual exposure and implementing measures such as network segmentation and network and endpoint security controls to prevent unauthorized access.

SKYBOX SECURITY

> "Given the importance of critical infrastructure to national security and America's way of life, accessible OT assets are an attractive target for malicious cyber actors **seeking to disrupt critical infrastructure** for profit or to further other objectives."[6]

[4-5] Gartner, *Market Guide for Operational Technology Security,* Katell Thielemann, Wam Voster, Barika Pace, Ruggero Contu, January 13, 2021.

[6] *Rising Ransomware Threat To Operational Technology Assets,* CISA, June 2021.

Operational technology under siege

Security experts have warned for years that OT systems were sitting ducks and that it was only a matter of time before they came under widespread assault. Now those predictions have come true. Recent years have seen an alarming rise in attacks on critical infrastructure and other OT systems. These breaches can inflict actual physical damage and disable systems that companies and society as a whole depend on, threatening not only bottom lines but also life and limb.

Here are just a few of the more notorious OT-focused exploits so far this year:

+ The attack in February on a water treatment plant in Oldsmar, Florida, where hackers attempted to poison the water supply with sodium hydroxide (lye).
+ The ransomware attack linked to the Russia-based DarkSide cybercrime ring that shut down the Colonial Pipeline in May, resulting in temporary fuel shortages and panic buying in the southeastern U.S.
+ The June ransomware attack by another Russia-based organization, REvil, on the world's largest meat processor (JBS), interrupting operations.

In all of these cases, as well as many other OT attacks, the hackers gained initial ingress through compromised assets, then moved across networks to penetrate sensitive OT systems. If proper network segmentation had been in place, that sort of lateral movement would have been blocked and the attackers stopped in their tracks. It's therefore crucial that organizations use tools designed to validate segmentation to ensure that vulnerable OT assets are not exposed.

Cybercriminals are all too aware that OT systems are ripe for the picking, and that ransomware attacks on those systems have a high likelihood of paying off. Companies simply can't afford to have these essential systems disabled, so they're often willing to pay large sums to keep them online. The National Security Agency (NSA) and CISA warned: "Over recent months, cyber-actors have demonstrated their continued willingness to conduct malicious cyber-activity against critical infrastructure by exploiting internet-accessible OT assets."[7] In fact, OT security has been elevated to a matter of national security by federal authorities. The Biden Administration's Executive Order on Improving Cyber Security, issued in May 2021, explicitly calls out OT—"the vital machinery that ensures our safety"—as an area that must be addressed.[8]

[7] *NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems,* CISA, July 23, 2020.

[8] *Executive Order on Improving the Nation's Cybersecurity*, whitehouse.gov, May 12, 2021.

More vulnerabilities exploited in the wild

As new security weaknesses emerge, threat actors are moving quickly to take advantage of them. The number of new vulnerabilities exploited in the wild grew 30% in H1 2021 compared to the same period last year. Interestingly, a growing percentage of these exploits (13% in H1 2021 versus 8% in 2020) are specifically targeting vulnerabilities rated as medium-severity on the CVSS scale.

This is a reminder that CVSS severity is not equivalent to risk. Many cyberattacks focus on weaknesses that are rated as less severe, exploiting these vulnerabilities as the first step in multistage attacks. Threat actors can take advantage of the fact that low- and medium-severity flaws often get less attention from security teams, using them to get a foot in the door and then stepping laterally through the network to gain deeper access. The salient point is that severity isn't the most important factor in measuring risk; it's *exposure*: the degree to which a vulnerability is or isn't accessible to attackers. Unfortunately, many vulnerability assessment tools lack effective exposure analysis.

Along with medium-severity vulnerabilities, attackers are also increasingly targeting local access vulnerabilities, which doubled as a share of the exploits in the wild relative to remote access vulnerabilities.

New vulnerabilities
exploited in the wild

+30%

From H1 2020 to H1 2021

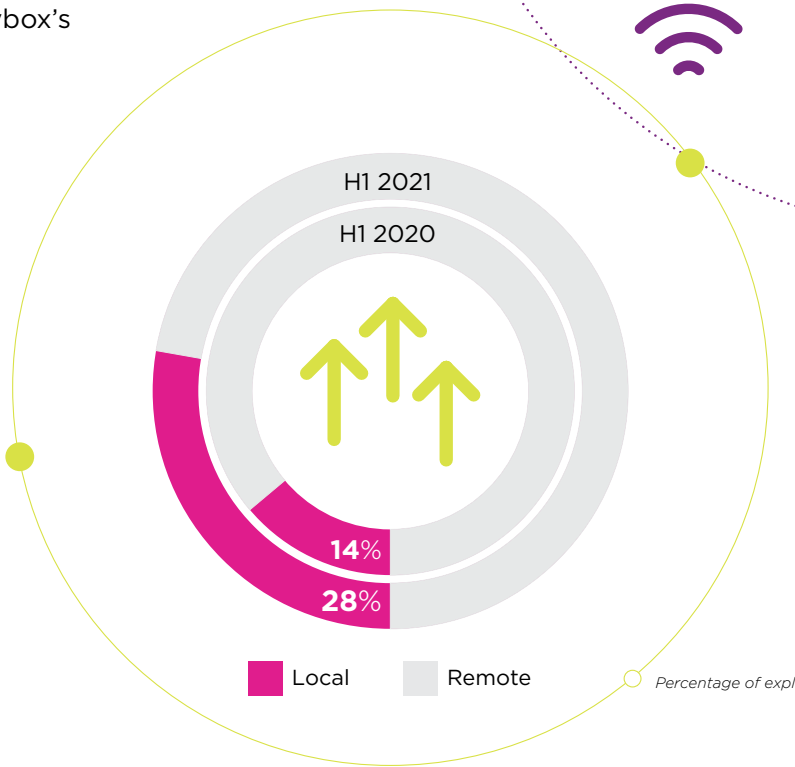
What is exposure analysis?

Exposure analysis identifies exploitable vulnerabilities and correlates this data with an enterprise's unique network configurations and security controls to determine if the system is potentially open to a cyberattack. This includes path analysis, used to ascertain which attack vectors or network paths could be used to gain access to vulnerable systems. Exposure analysis is only possible when disparate data repositories are normalized and brought together into a network model, including patch and asset management systems, vulnerability data, threat intelligence feeds and cloud and network device configurations.

Some of this growth may be due to an increase in VPN attacks, which enable external threat actors to gain local access to networks. There was an explosion in the use of VPNs last year, as companies scrambled to support more remote workers during the COVID-19 pandemic. The hasty rollout of VPNs led to configuration errors and other security failures that opened the way to breaches. Vulnerabilities in VPN products contributed to the problem. For example, there was a 1,916% increase in attacks against Fortinet SSL-VPN devices and a 1,527% increase in attacks against Pulse Connect Secure VPN last year.[9] This year, Cisco RV routers—which include VPN functionality—made their first appearance in Skybox's top ten list of products with the most vulnerabilities (see chart: "Products with the most new vulnerabilities").

> "[VPNs] continue to be targeted by a plethora of threat groups, which will almost certainly continue for the remainder of 2021. VPN devices, in addition to other remote access software, are often prioritized as a useful entry point that can provide threat groups with a stable foothold onto target networks."[10]

Vulnerabilities
by access vector



Percentage of exploits in the wild: local vs remote

[9] *Q1 2021 Threat Landscape Report,* Nuspire, 2021.

[10] *Attackers Heavily Targeting VPN Vulnerabilities,* Dark Reading, April 21, 2021.

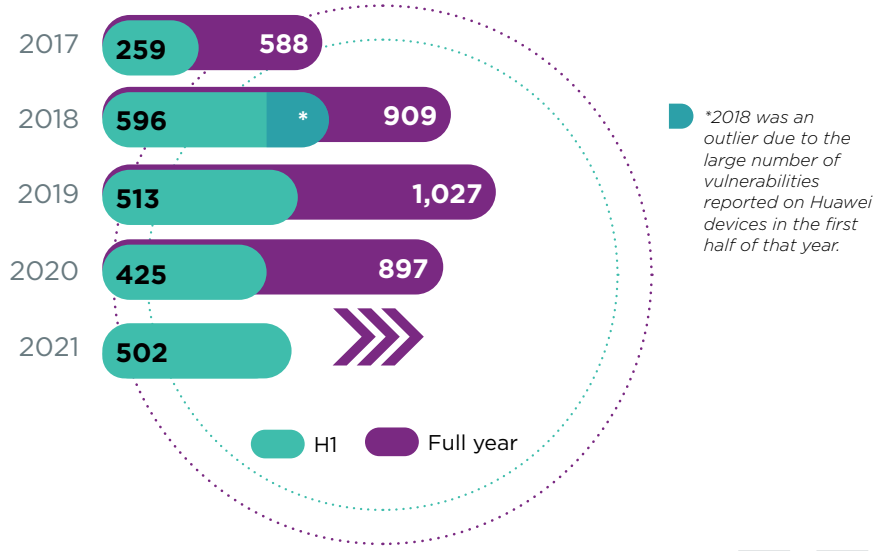
Network device vulnerabilities in the crosshairs

The number of vulnerabilities in network devices such as routers, switches, firewalls and their operating systems rose nearly 20% in H1 2021. Last year's decrease in new network device vulnerabilities, described in our previous Vulnerability And Threat Trends Report,[11] appears to have been a temporary dip, and this year's uptick likely signals a return to the growth pattern of previous years.

Like OT, network devices are an Achilles heel for many organizations. These devices are critically important parts of the infrastructure, yet their security flaws are often invisible because network devices are difficult or impossible to effectively scan. Scanning can impact performance or even shut down systems, and is further complicated by the need for special passwords and access privileges.

It's ironic that devices designed to bolster security, such as firewalls and VPNs, are introducing new weaknesses and blind spots into networks. The vulnerabilities are often widespread, popping up repeatedly in affected devices. For example, a critical vulnerability was reported earlier this year in BIG-IP server appliances from F5 Networks.[12] These appliances perform tasks such as load balancing and DDOS (distributed denial of service) mitigation. Some enterprise networks have thousands of these appliances in use. Patching all of them would be enormously time-consuming and costly. It would also be a monumental waste of effort, since it's typically just a small subset of such devices that are actually exposed to attack. Fortunately, sophisticated risk assessment tools that use exposure analysis can identify the specific assets in need of immediate remediation, narrowing the to-do list from thousands of devices to just a dozen or fewer in some cases. That's a huge reduction in complexity and an order of magnitude better than legacy risk assessment tools that lack exposure analysis.

New vulnerabilities in network devices over 5 years



[11] *Skybox Vulnerability And Threat Trends Report 2021,* Skybox Security, February 2021.

[12] *Hackers are exploiting a server vulnerability with a severity of 9.8 out of 10,* ars technica, March 19, 2021.

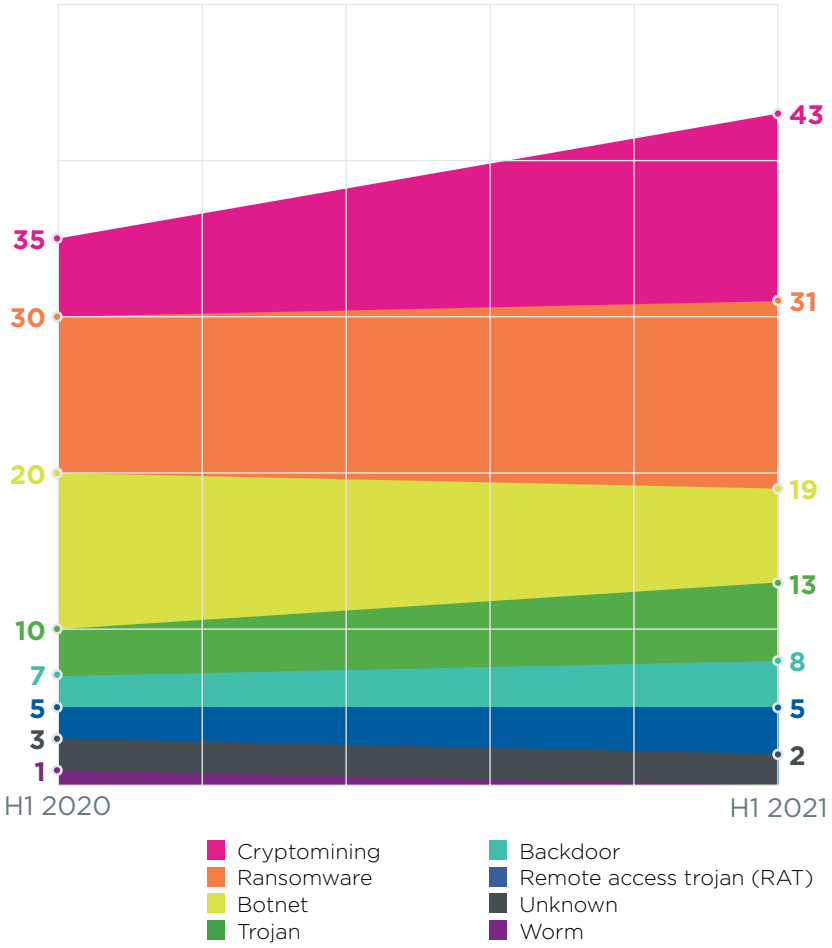
Cryptomining tops the charts in new malware growth

The number of recognized malware programs exploiting new vulnerabilities grew 20% relative to H1 last year. Malware increased in almost every category we measured.

Malware programs used for surreptitious cryptomining took the lead, more than doubling in comparison to H1 2020. This malware hijacks computing power to mint new cryptocurrency such as bitcoin. Cryptomining is a potentially lucrative activity, but the gating factor is the computation required to mine bitcoin and some other cryptocurrencies. That process is getting more difficult and resource-intensive, which is why unscrupulous miners are increasingly turning to malware to poach computing power inside enterprise networks. Malware vendors are only too happy to assist, providing exploit kits designed for cryptomining. Often recoding existing malware to serve this purpose. In some cases, malware-as-a-service providers lease botnets composed of already-infected machines to cryptominers.

New malware exploiting vulnerabilities

H1 2021 vs H1 2020

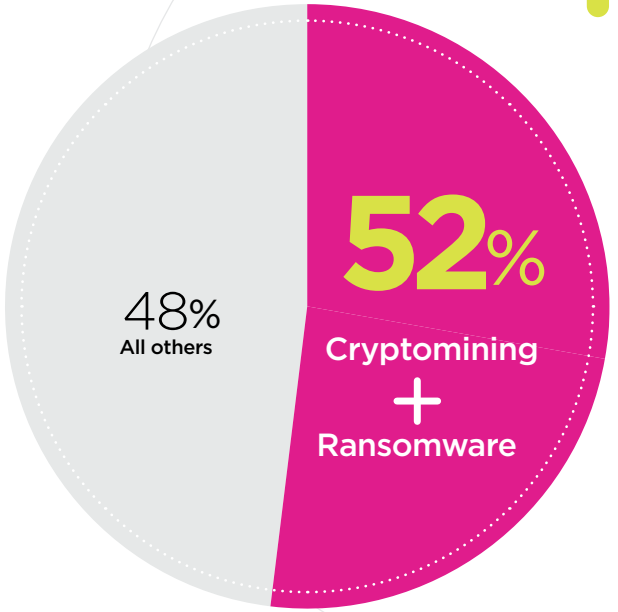


Malware **increased** in almost every category we measured.

> We found that **69% of organizations** experienced some level (at least one end-user instance) of unsolicited cryptomining."[13]

In response to the cryptojacking threat, enterprises must not only get better at preventing infection in the first place, but also at implementing and enforcing policies that cordon off infected machines and prevent them from exfiltrating data. This requires identifying potential ingress and egress paths and ensuring proper configuration, access controls and measures such as network segmentation.

Another malware category that grew in H1 2021 is ransomware. This increased by 20% versus the first half of 2020. Given the increasing popularity and profitability of ransomware attacks, it's likely that this class of malware will continue to grow in the years ahead.[14]



New malware

exploiting the highest number of vulnerabilities

[13] *2021 Cybersecurity threat trends: phishing, crypto top the list,* Cisco, 2021.

[14] *Why ransomware attacks are on the rise—and what can be done to stop them,* PBS, July 8, 2021.

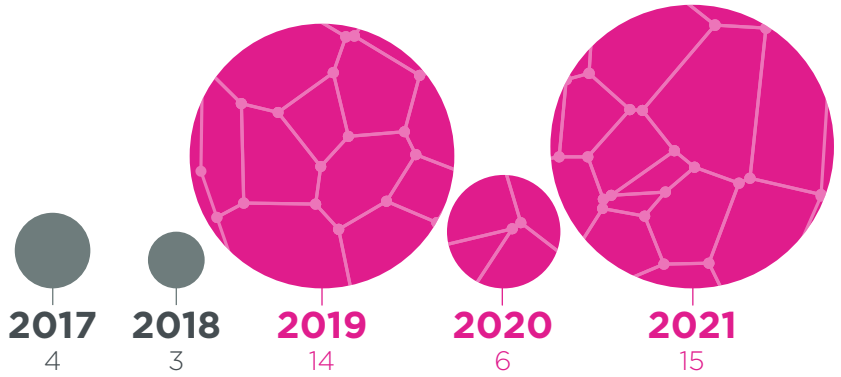
Not only are cryptomining and ransomware two of the fastest-growing malware categories, but they also exploit the greatest variety of vulnerabilities—more than all other categories of malware combined. By creating programs that exploit an array of vulnerabilities, malware providers can serve a wider range of customers with a single product. These versatile programs are like Swiss Army knives, multipurpose tools that can be used for a range of exploits.

Interestingly, we found that new malware overwhelmingly exploited more recent vulnerabilities (vulnerabilities reported in the last three years).

This clearly indicates that malware creators have new vulnerabilities on their radar, and are actively developing novel malware to take advantage of the latest weaknesses. Often this is accomplished by simply tweaking existing malware to perform new exploits. In effect, malware evolves like viruses, with new variants springing up opportunistically in response to a changing environment.

Malware evolves like viruses, with new variants springing up opportunistically in response to a changing environment.

New malware is
targeting recent vulnerabilities



Number of vulnerabilities exploited by new malware, by publication year

Modernizing vulnerability management

If the findings in this report make one thing clear, it's that traditional approaches to vulnerability management are falling further and further behind. Too many assets, including OT and network devices, are difficult or impossible to scan. Vulnerabilities are too numerous, threats too varied and infrastructure too complicated (fragmented, siloed and heterogeneous) to assess using conventional, largely manual processes. Finding and patching all vulnerabilities is simply out of the question, and the criteria typically used to prioritize remediation efforts are too broad—missing many real threats while wasting time on false positives.

As a result, IT and security teams are caught in a vicious cycle, spending more money and resources on increasingly ineffective measures, while failing to keep pace with the rapidly evolving threat landscape.

Enterprises require solutions that provide comprehensive visibility across their entire network, that precisely identify the most salient threats and that facilitate timely, cost-effective remediations. Specifically, organizations need:

1 Vulnerability discovery: beyond active scanning

Disconnected discovery methods and intermittent scanning produce a very incomplete picture. To provide more comprehensive coverage, discovery needs to go beyond scanning and incorporate data from configuration, patch and asset management systems; endpoint security systems; threat intelligence feeds; and a variety of other assets including cloud, OT and network security devices. This form of data collection, sometimes referred to as "passive scanning," can be combined with active scanning to create a single continuous and holistic view of the entire attack surface.

2 Exposure analysis: beyond limited risk scoring

Traditional risk scoring has a glaring gap. While factoring in things like severity, asset importance and exploitability, it neglects the most important variable of all: exposure. No matter how severe or exploitable in theory a vulnerability is, it can't be attacked if it's not exposed.

On the other hand, even a low- or medium-severity vulnerability can pose a serious risk if it's readily accessible to threat actors. Increasingly, attackers use such seemingly innocuous vulnerabilities as the first step in sophisticated multistage campaigns. Once they've gained entry through these back doors, intruders move laterally through a network to attack more sensitive assets. That's why exposure analysis is the essential component of threat-centric risk assessment.

Exposure analysis consists of complete path analysis (analyzing all the paths to and from IT and OT assets) and attack simulation to show all the potential ways threat actors can get to an asset. This is only possible if you have a comprehensive network model that understands your entire hybrid network, including OT, hybrid and multicloud (see sidebar: "What is exposure analysis?").

3 Optimal remediation: beyond patching

Once exposure analysis has been used to identify and prioritize the most pressing security threats, organizations need practical ways to remediate problems and protect their networks. And since patching isn't always feasible, that means taking other measures: adjusting configurations, enforcing appropriate policies, applying IPS signatures, implementing network segmentation and more. In so doing, security teams can ensure that assets—even those with unpatched vulnerabilities—are fully protected and not exposed. This is particularly important for areas such as OT and network devices, providing a way to secure these assets without downtime and other operational impacts. Advanced solutions can help to optimize this process, automatically suggesting the most effective remediations to reduce risk.

Combining these three elements (comprehensive vulnerability discovery; exposure analysis; and optimal remediation) provides the intelligence and context security teams need to efficiently identify and address the most dangerous and urgent threats in need of immediate remediation and avoid wasting time trying to chase down every vulnerability. For enterprises that want to fortify their organization while streamlining processes and harnessing new efficiencies, **that's a big win-win**.

Methodology

All of the findings in this report, unless otherwise noted, are based on data from Skybox Research Lab, the threat intelligence division of Skybox. The Skybox Research Lab has been at the forefront in analyzing the latest cyber vulnerabilities and threats for over a decade. The lab delivers comprehensive, actionable and timely threat intelligence that powers Skybox's vulnerability and threat management solution and enables our customers to discover, prioritize and remediate risks.

Our team of security analysts continuously monitors dozens of security sources, tracking and analyzing tens of thousands of vulnerabilities on thousands of products, along with the latest data on exploits and malware taking advantage of these vulnerabilities. Drawing on this research, the team identifies the vulnerabilities most likely to impact our customers' networks and assets. These vulnerabilities are combined with critical contextual information on whether and how the vulnerability has been exploited, the prevalence of the vulnerability, the malware that exploits it, the damage it can inflict and optimal approaches to remediation. All of this information is incorporated in a proprietary database used in our product and by Skybox customers.

The Skybox database has information on more than **130,000 vulnerabilities** in roughly **14,000 products**, including:

+ Server and desktop operating systems
+ Business and desktop applications
+ Networking and security technologies
+ Developer tools
+ Internet and mobile applications
+ IIoT devices
+ Industrial control system (ICS) and supervisory control and data acquisition (SCADA) devices

Most of the statistics and findings in this report are based specifically on the intelligence in the Skybox database. In a few cases we've used other sources such as the NVD instead, as explained below.

Overall vulnerabilities

Overall vulnerability counts are based on new vulnerabilities reported in the NVD. The age of vulnerabilities is based on the publication date in the NVD. For example, vulnerabilities are counted as "new" in H1 2021 if they were published in the NVD during that period.

OT vulnerabilities

When counting OT vulnerabilities, we consult the Department of Homeland Security's Industrial Control Systems Emergency Response Team (ICS-CERT), the most authoritative source of OT vulnerability data. The OT vulnerabilities in this report are based on new vulnerabilities shared in ICS-CERT in H1 2021.

New malware

To identify any new malware, our security analysts continuously monitor new cybersecurity advisories and other sources. The data on the rise of malware in this report is extrapolated from these daily intelligence feeds.

Vulnerability severity

The vulnerability severity rating used in this report is part of our risk modeling methodology (CVSS V3 compliant), which takes a variety of parameters into account. The CVSS base score ranges from 0 to 10.

Network device vulnerabilities

To track network device vulnerabilities, we specifically looked at vulnerabilities in firewalls, routers, switches, network appliances and their operating systems. We deliberately excluded other OT systems such as cameras and industrial control systems, since those are covered separately in the OT section of this report.

Exploits by access vector

To define access vectors as local or remote, we followed the CVSS 3.1 specification guide. We also counted physical access as local and adjacent network access vectors as remote.

Exploits in the wild

When counting new exploits in the wild, we've focused specifically on exploits targeted at new vulnerabilities, drawing on the intelligence collected in the Skybox database.

About Skybox

Over 500 of the largest and most security-conscious enterprises in the world rely on Skybox for the insights and assurance required to stay ahead of dynamically changing attack surfaces. At Skybox, we don't just serve up data and information. We provide the intelligence and context to make informed decisions, taking the guesswork out of securely enabling enterprises at scale and speed.

Our security posture management platform delivers complete visibility, analytics and automation to quickly map, prioritize and remediate vulnerabilities across your organization. The vendor-agnostic platform intelligently optimizes security policies, actions and change processes across all corporate networks and cloud environments. With Skybox, security teams can now focus on the most strategic business initiatives while ensuring enterprises remain protected.

Interested in speaking with an expert to help solve your greatest security challenges?

Contact us.

skyboxsecurity.com

SKYBOX SECURITY