Report

Emerging External Cyber Defense Trends

BlueVoyant

Executive Summary

As enterprises' internal cybersecurity has become more well-defended and better monitored, cyber threat actors have evolved their tactics to focus on new methods of compromise, targeting a wider attack surface than ever before. What that practically means is that organizations need to look outside their traditional IT perimeters to understand the full scope of threats that can result in a cyber incident.

To gain a greater understanding of this extended attack landscape, BlueVoyant continuously analyzes the latest external threats, vulnerabilities, and risks. This includes all threats from outside of organizations' internal networks, such as those that come from suppliers, vendors, and other third parties, along with threats further outside the wire on the clear, deep, and dark web.

In the following report, we have cataloged insights both on increasingly prevalent attack vectors as well as remediation and mitigation advice on relatively straightforward ways to defend against them. For instance, the alarming rate of emerging vulnerability disclosures poses a threat to virtually all organizations, but whose risk can be greatly reduced with the relatively simple fix of patching as quickly as possible.

The evolution and adaptation of threat actor tactics, techniques, and processes continue to pose a challenge for threat hunters and analysts to track and monitor threat actor communications, and the purchase and sale of stolen payment cards. Instant messaging offers threat actors a more reliable way to communicate than dark web forums, though these methods are not impossible to intercept if analysts know how to look for them.

Being aware of these trends can help organizations across all sectors better defend themselves against a continually changing landscape. For that reason, in addition to trends, we have also supplied advice on mitigation strategies, which we hope can be taken advantage of and applied to benefit our vastly interconnected modern business ecosystem.

Overview

External Cyber Defense and its Growing Importance

One of the primary cybersecurity challenges faced by organizations today is an expansion of the digital ecosystem that must be overseen and defended. Networks are larger than ever before with an enormous growth in external web presence and outside dependencies. The COVID-19 pandemic has resulted in major shifts in working culture, with an increase in remote workers and the technology needed to serve them. These technologies, often deployed at scale, have increased the probability of vulnerable accounts and services connected outside an organization's core network.

As a result, it has become harder to identify basic externally facing vulnerabilities and threats due to sheer volume, and threat actors are increasingly taking advantage of these exposures, pivoting and evolving their tactics to achieve their goals.

To address this change in business processes and counteract the growing threat of compromise to the external attack surface, there is an increasing need for organizations of all sizes and across all sectors to give greater consideration to External Cyber Defense — the action and process of remediating and mitigating threats that can target an organization's web presence as well as extrinsic, third-party connections.

To shed light on the state of external cyber defense, BlueVoyant has compiled the following analysis of emerging trends that represent critical concerns for organizations of all types. This analysis is based on BlueVoyant's observations and data collection, derived from its continuous monitoring and mitigation of threats to its client's extended ecosystems.

This analysis is based on the perspective of threat actors and what they might look to most broadly exploit. This means focusing not only on findings and vulnerabilities, but also looking in depth at attacker tactics, techniques, and procedures.

A common thread across all trends concerning external defense is that timeliness is critical to mitigating the risks of the threats herein profiled. As such, the primary objective of this report is to empower readers to be "threat informed" so that they have the knowledge to take effective action quickly.

Below we take a look at several trends that BlueVoyant has observed impacting the state of external cyber defense, as well as the takeaways and responses that such trends should elicit in organizations looking to protect themselves.

Trends and Observations

1. Increasingly Advanced and Dynamic Phishing Tactics

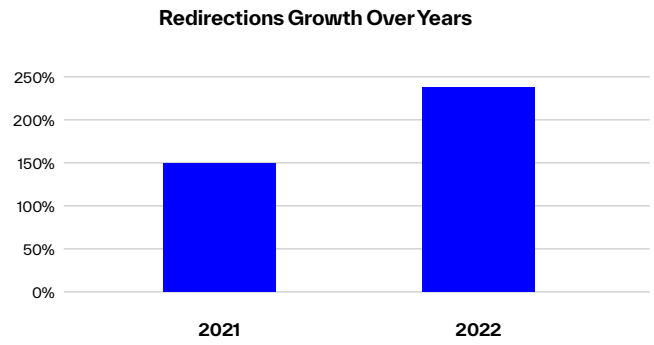
The COVID-19 pandemic forced global business to accelerate their digital transformation initiatives in an abrupt manner. As employees were relegated to working from home and storefronts around the world shut their doors for weeks, months, or even years in some parts of the world, the economy became more reliant on digital transactions than ever before. This meant more cloud hosting, more adoption of mobile apps and investments in web presences, and, ultimately, more potential attack vectors for hackers to exploit.

And exploit them they did. BlueVoyant's analysts have observed increasingly sophisticated phishing tactics that prey on the weakest link — the end user. Hackers have always searched for new and innovative ways to execute attacks against companies and their users, but they accelerated their efforts in response to the newly remote workforce and primarily digital global economy. The following examples are three of the many tactics threat actors have used over the past year:

Tactic 1: Phishing Link Redirections

One of the more complicated ways threat actors evade detection involves multiple redirect paths, steering consumers to spoofed domains while redirecting presumed threat hunters or phishing analysts to an error page. These evasion mechanisms include User Agent or IP restrictions and blocklisting, with significant emphasis placed on bot and crawler detection. The purpose of this type of redirection is to hide the phishing content on a single website by diverting threat hunters elsewhere, i.e. the target's official domain, a google search, etc.

The following chart demonstrates the year-over-year increase in phishing attacks using redirections in 2021 (150%) and 2022 (240%):



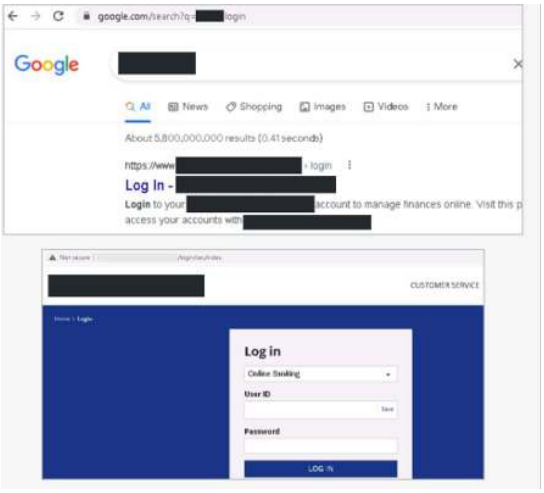
After clicking on a phishing link, users are redirected to another site, sometimes utilizing multiple "hops" and redirecting across several domains until they finally reach the destination phishing site. This poses a challenge to threat hunters and phishing detection platforms, which, if categorized by the threat actor's code as a bot or crawler, are prevented from accessing the phishing page.

Another type of redirection aims to distribute the activity across several domains in the redirection chain to make detection harder by sending some victims to one domain, while the actual phishing content is in fact on a second domain.

When dealing with this type of redirection, the threat hunter's location and operating system can be a factor. From certain IP addresses or mobile devices, a phishing site could automatically block access to the malicious site. The website might initially display a directory tree, which includes the path supposedly containing the phishing content. Clicking the path, however, does not lead to phishing content, and instead either displays an HTTP 403 error message, redirects to a seemingly benign Google search of the target name, or redirects to the target's official website.

To reach the phishing page, a threat hunter will need to add another path segment that differs from kit to kit and could be altered by the threat actor. This technique is highly effective in thwarting cyber threat analysts from detecting the phishing content while displaying the correct URL to the victims.

The below image depicts a subdomain impersonating a large US bank. Upon entering the website, the user is instantly redirected to a Google search of the bank's name. Adding the path "/login/ses/index" leads to the live phishing content impersonating the bank.

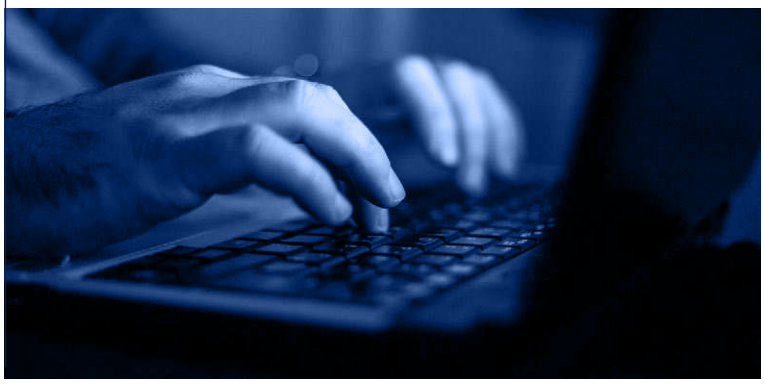


Tactic 2: Leveraging Dynamic DNS Infrastructure

Dynamic DNS hosting providers are particularly popular among threat actors because they provide a convenient platform to easily set up and host multiple phishing pages without having to register a domain. BlueVoyant has been tracking phishing activity leveraging this infrastructure since 2021, and found that 67% of all phishing attacks were hosted on dynamic DNS infrastructure by the end of that year, demonstrating the infrastructure's quick adoption and massive scale of use.

Many novice threat actors turn to phishing to score a quick profit despite their lack of technical proficiency and resources to create and set up their own websites. The affordable price of readily available phishing kits and the conveniently free dynamic DNS Infrastructure create the perfect gateway for new hackers to enter the game.

The lifespan of phishing websites on dynamic DNS Infrastructure is relatively short, with pages lasting one or two days on average. What it lacks in durability, the infrastructure makes up for in quantity: there are thousands of new active phishing subdomains per day, resulting in thousands of compromised accounts. For threat actors concerned with carrying out the most successful attacks for the least amount of money in the shortest time frame, this vector provides an excellent opportunity for a low-cost, high-volume campaign that can be duplicated (or slightly altered) in future attacks — all without having to register a domain.



Tactic 3: Smishing

The use of SMS text messages as a platform to distribute phishing messages — known as "smishing" — is steadily increasing, affecting millions around the world and causing severe financial losses. BlueVoyant analyzed the process and tools used by threat actors to perform a smishing attack, types of smishing messages, and the intersection of smishing with the Dynamic DNS Infrastructure, a platform largely abused by threat actors to host a large volume of phishing websites.

The majority of smishing messages contain an external link leading to a phishing website. As such, threat actors must first obtain a phishing kit, a domain, and a web hosting platform to get their malicious website up and running. As smishing gains popularity, many kits are coded and advertised as mobile-compatible. For mobile users, the phishing website will appear legitimate and authentic. In addition to mobile compatibility, some kits are configured to be accessible only via mobile based on the user agent. This restriction makes the websites much harder to detect, allowing them to remain online for longer than average, resulting in more victims.

To carry out a successful smishing attack, threat actors require an automated tool that can send SMS messages in bulk. SMS gateway scripts are sold on the deep and dark web as all-inclusive solutions, which are rather easy to operate, and require very little technical knowledge. The user is typically only required to provide the following parameters:

- **Sender phone number:** obtained by either using VoIP services, such as Google Voice, or by linking the user's actual mobile device
- **Recipient phone numbers:** the smishing victims
- **Message content:** the social engineering message and malicious link

Once the user inputs this data, the gateway script often connects to a third-party gateway API to perform the SMS delivery on the backend. This means that legitimate SMS gateway providers, which are catered toward digital marketing and customer relationship management, are abused by threat actors to deliver smishing messages.

Takeaways and Recommendations

As global business continues to embrace digital transformation, security teams will face a never-ending onslaught of new phishing attack techniques. Ensuring your organization is best positioned to withstand and thwart those attacks is a critical priority.

Make sure that your digital risk management vendor has the capabilities to circumvent redirections and identify phishing domains. To protect against large-volume phishing attacks, it is important to maintain daily monitoring for newly created subdomains leveraging dynamic DNS infrastructure. Quick detection and remediation are crucial to shutting down these attacks at the source.

To mitigate the threat of smishing, it is important to guide your clients to be vigilant and report cases. Smishing is a symptom and not the problem itself. The ideal is to have suspicious phishing sites taken down before they reach the target via SMS, so make sure you are well protected against brand impersonations. Transfer your abuse box to your digital risk protection vendor, which should be able to remediate cases reported by clients.

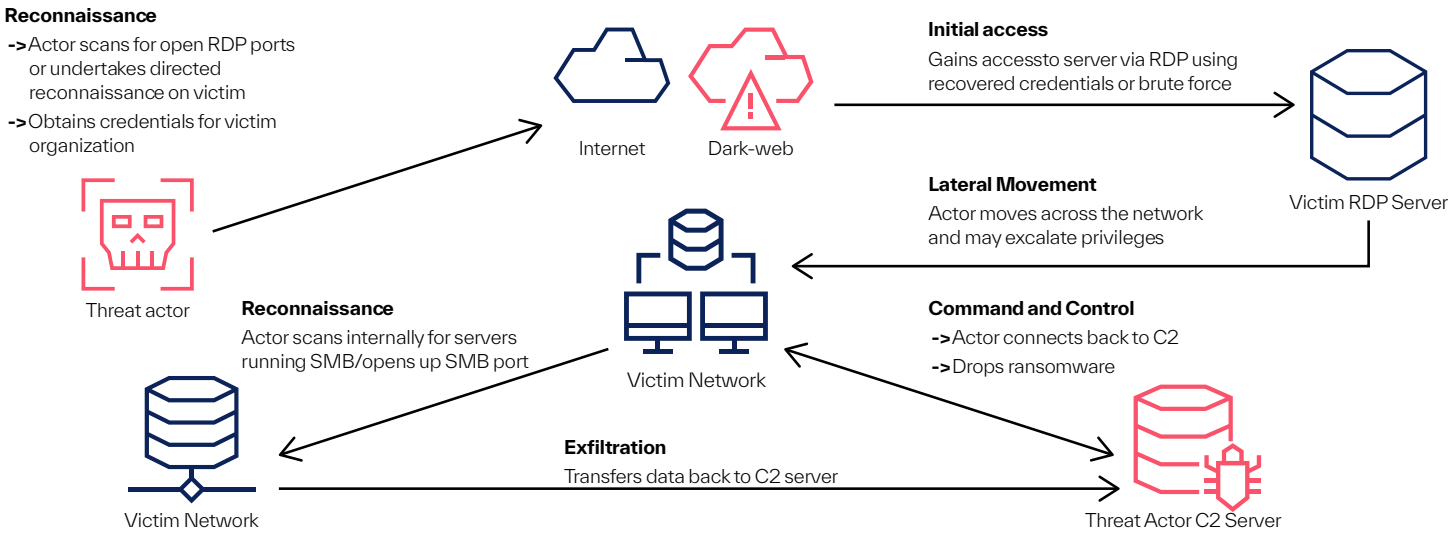
2. RDP as a Primary Vector for Ransomware

Overview

With the ever-increasing need for external remote network access, and the rise of third-party connectivity, supporting technologies widely adopted by modern organizations continue to pose a greater risk and are increasingly being targeted by threat actors. Protocols like RDP, SMB, and WinRM can facilitate important business processes but introduce increased risk that must be considered in any security analysis. The Remote Desktop Protocol (RDP) in particular, has been observed as a service with increasingly successful and effective exploitation.

RDP, the proprietary Microsoft protocol that allows a user on one computer to connect to and control a remote computer, is commonly used by admins to fix an issue on a remote system, and in recent years has become popular for cloud computing to access and/or manage virtual machines in the cloud environment. Unfortunately, it is very easy to expose RDP unintentionally by leaving the RDP port open to the internet, including on a forgotten system, cloud instance, or network segment. This protocol, easily detected and exploited, can lead to loss of data, downtime, costly remediation, and brand damage for organizations.

In recent years, threat actors have more frequently probed for open RDP ports as an easy-access attack vector, since they can find vulnerable open RDP services by simply running an external scan of an organization's network. It is a foregone conclusion that RDP will be targeted at some point if left open on an organization's network.

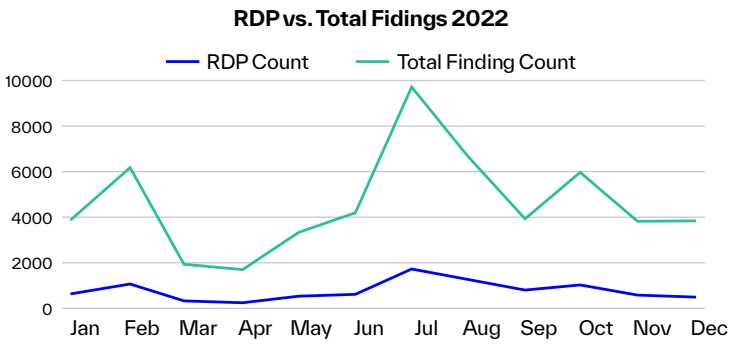


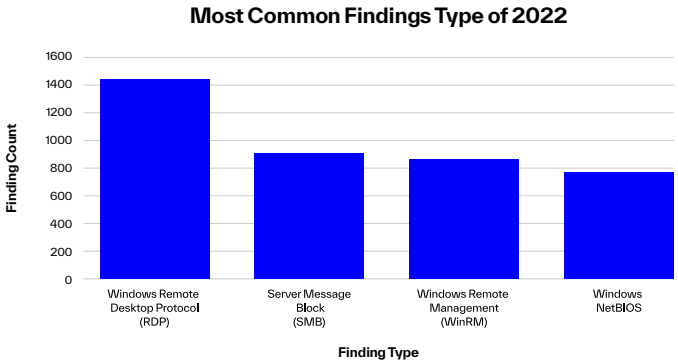
According to CISA[1], in 2021, RDP was one of the top three initial attack vectors for ransomware events, often involving either brute force or stolen credentials for access. Additionally, The COVID-19 pandemic has contributed, in a unique way, to the increase in RDP targeting, due to the uptick in remote work. The heavy demand for remote access technologies to support work and schooling from home has quickly expanded the attack surface of many organizations leaving these exposed services ripe for the picking. RDP requires authentication so an attacker does need credentials, but weak passwords, poor operational security and increasingly effective credential harvesting campaigns, make the acquisition of RDP credentials easier than it should be.

Observations

Based on our view of risk indicators, BlueVoyant can confirm the trend of internet-exposed RDP services. A notable number (on average approximately 20%) of the risk indicators detected in the third-party ecosystems (i.e. supply chain) of organizations are due to exposed RDP ports. Despite the fact that RDP risk has been warned about for years, it remains a primary access vector for attackers and continues to make headlines in cybersecurity news outlets.

In a sample of over 15,000 companies monitored from January 1 to December 31, 2022, 20% of vulnerabilities BlueVoyant analyzed within those companies were RDP-related. This is a consistent number month-over-month. More than 25% of companies monitored in that time were notified of at least one open RDP observation.





The high usage of RDP as an attack vector is comparable with the increased targeting of SMB and NetBIOS (other remote server communication services), both common vulnerabilities that BlueVoyant has observed in its analysis of organizations across all sectors and industries.

For the reasons laid out above, BlueVoyant continues to prioritize these kinds of findings, distinguishing them as critical even among other notable and more recent vulnerabilities observed. BlueVoyant highlights these indicators of risk that are widely recognized and publicized as being targeted by threat actors, and that are often an ingredient in immediate compromise and ransomware incidents.

Takeaways and Recommendations

Despite the prevalent and impactful threat of RDP exploitation, a simple remediation can be implemented to eliminate this attack vector and improve cyber risk posture. Resolution for risky RDP use includes the use of VPNs, limiting login attempts and multi-factor authentication among others. Yet most importantly is the simple awareness that an organization has the service exposed. Without a valid business reason, services such as RDP should be disabled and ports should be closed to the internet. The curation of RDP ports and their closure is consistently recommended as a cybersecurity best practice by national-level organizations and security frameworks.

Additionally, it's important to remember that any activity surrounding remote connection to company assets should be thoughtfully utilized and regularly audited by security teams.

3. Emerging Deep and Dark Web Financial Fraud Campaigns

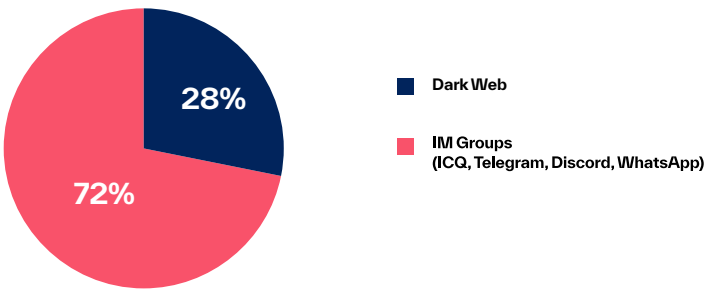
Cyber fraud certainly is not a new type of attack, especially when targeting financial organizations, but our analysts have started to see new wrinkles over the past year — threat actors gravitating toward private instant messaging platforms instead of the dark web, opting to utilize fraudulent physical checks in their campaigns, and business mule accounts being used to launder money successfully obtained via fraud campaigns.

Instant Messaging: The New Watering Hole

For many years, cyber threat activity was reliably found in various forums across the dark web. However, in an attempt to limit exposure to authorities and infiltration by threat hunters, prominent hackers have moved their operations to private instant messaging (IM) channels on encrypted platforms like WhatsApp, Telegram, etc. This complicates threat detection for businesses and cyber threat intelligence purveyors alike — penetrating exclusive, invite-only IM groups can be significantly more challenging than joining anonymous dark web forums that could be found by anyone with the Tor browser installed.

BlueVoyant has gained access to many of these secure IM channels using an automated mechanism that scrapes the content for the purpose of scaling. Our analysts have identified new and increasingly complex attack methods targeting large financial organizations as a major trend. The following chart demonstrates that IM cybercrime groups are now the primary destination to sell and purchase stolen payment cards:

Leaked Payment Cards Source Distribution

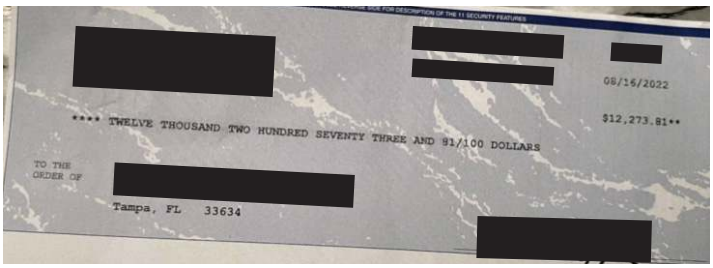


Physical Check Fraud

We have encountered numerous cases of threat actors selling physical checks for use in extended fraud campaigns, typically targeting businesses or other organizations that would presumably have liquid cash in their accounts. In the past, threat actors have primarily focused on digital cyber fraud campaigns — using stolen credit card numbers to purchase valuable goods on the internet or deposit money directly into an account that cannot be traced. But as cyber threat detection platforms have begun to catch up with these attack methods, some hackers have chosen to evade detection by going analog. Our team is working on further research on this new trend with the aim of publishing a full report in the coming months.

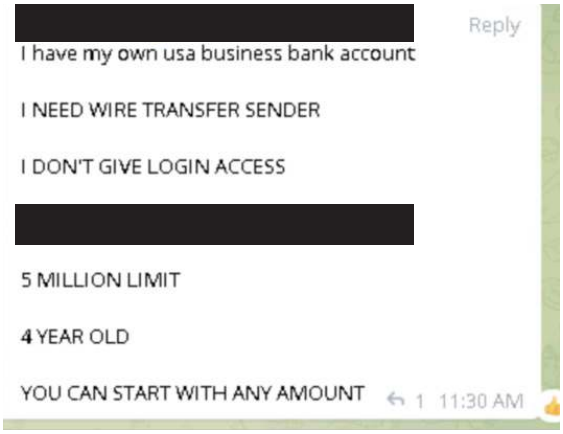
The tricky thing with physical checks is that they cannot be detected digitally, putting security teams at a disadvantage. The checks may have already been used or deposited by the time the affected business or person becomes aware of the fraud attempt. This means engaging directly with threat actors becomes all the more important, which must be done manually by experienced threat hunters who have earned the trust of a private IM group.

The following is an example of a physical check BlueVoyant identified in a Telegram cyber crime channel. It appears to be legitimate, impersonating a business and appearing to be issued by a major US bank:



Business Mule Accounts: High-Dollar Repositories for Scam Artists

BlueVoyant analysts have observed an increase in threat actors offering up business banking accounts to serve as mules in fraud-related money laundering schemes. As part of our continuous monitoring, our harvesting system identified a message posted by a threat actor in an underground Telegram group claiming to have a business mule account with a major US bank. The threat actor added that the account is four years old and can receive wire transfers of up to $5 million (the advantage of having a business account vs. a personal account). BlueVoyant analysts have actively engaged with the threat actor and were able to obtain the details of the suspicious account, seen below.



Takeaways and Recommendations

Security teams face a serious threat intelligence challenge as threat actors outmaneuver them on private IM channels. Monitoring the deep and dark web to identify IM groups that may share information about your organization can position your team to gain access to certain private groups over time. As your team develops cybercrime avatars and contributes to group discussions, they can become trusted members of the hacking community and gain access to exclusive intelligence.

Furthermore, it should be common practice to perform routine security check ups such as password resets. Make sure your security vendors prioritize developing and expanding their monitored sources, to provide adequate and comprehensive coverage.

Given the incisive threat posed by check fraud, It is important to monitor the deep and dark web to identify compromised checks as they become available, and flag and block related checks, as well as secure the compromised checkbook. In parallel, as mule accounts can appear legitimate upon first glance, organizations must passively monitor the deep and dark web and actively engage with threat actors to obtain mule account details. Following this, security analysts must monitor and analyze the account's activity for any patterns which may assist in proactively detecting mules in the future. This underlines the need for a proactive approach in counteracting fraud in general.

4. The Prevalence of Zero-Day Vulnerabilities and their Patching Cadences

Overview

Zero-day vulnerabilities, also referred to as Emerging Vulnerabilities (EVs), represent one of the most notable threats to organizations due to their unforeseen and time-sensitive nature. New EVs are disclosed each week, and companies across the world and across all industries need to be constantly vigilant of which can affect them. One of the major challenges in reducing risk in an extended ecosystem is ensuring that all organizations and suppliers do not have open, unpatched instances of vulnerable software, especially when considering that the average time to compromise for a newly disclosed Zero-Day is only around 2 weeks or less.

Through its continuous monitoring service, BlueVoyant rapidly identifies EVs within its global dataset made up of the external-facing IT Infrastructures of organizations from all industries and sectors. It is able to signal detections of specific assets within corporate entities. By leveraging this capability, in the following cases, BlueVoyant signatured the vulnerabilities in question and captured the remediation rate for all organizations within its data, in addition to our own clients. From this BlueVoyant can draw a number of conclusions about how companies respond to the disclosure of new EVs.

Observations

To give an idea of how frequently emerging vulnerabilities are disclosed, in only a single quarter of 2022 (Q4), BlueVoyant observed, signatured, and notified companies regarding the following EVs:

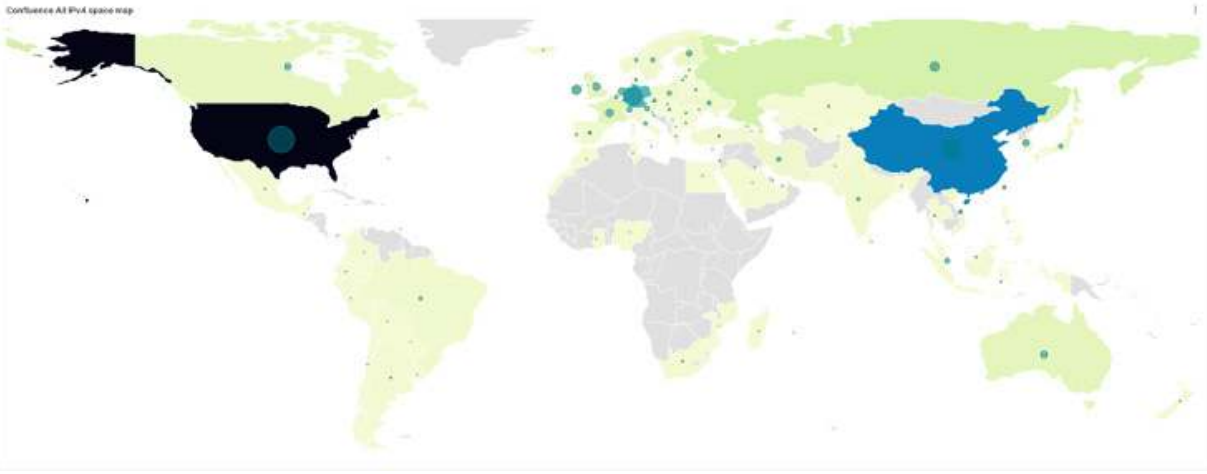
EV Description	Date
Fortigate Firewall Severe Authentication Bypass Issue, October 2022	Oct 2022
Aruba Critical EdgeConnect RCE and Auth Bypass Vuln	Oct 2022
Palo Alto Auth Bypass	Oct 2022
Zoho ManageEngine	Oct 2022*
Citrix Auth Bypass	Nov 2022
FortiOS SSL-VPN	Dec 2022
Citrix ADC	Dec 2022

BlueVoyant can illustrate trends in patching with the following two separate and distinct examples of how disclosures can impact company actions to mitigate risk:

1. Atlassian Confluence - Confluence Data Center and Server CVE-2022-26134

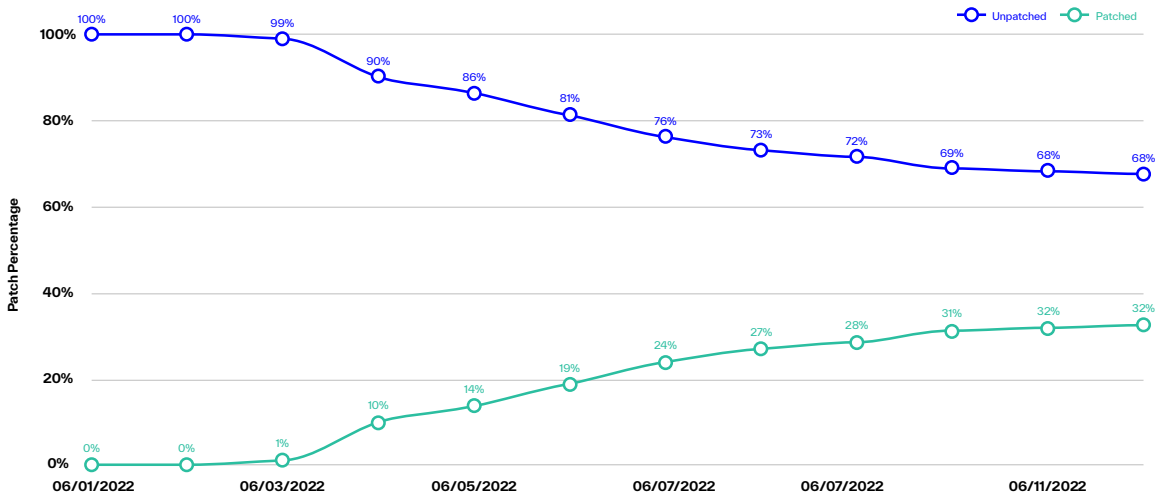
On June 2, 2022, Atlassian announced[2] that it had been made aware of an active vulnerability present in its Confluence Data Center and Server software, now classified as CVE-2022-26134.[3] Atlassian Confluence is a collaboration tool, according to the company.[4]

In the case of CVE-2022-26134, BlueVoyant signatured the vulnerability and captured the remediation rate for all client vendors within our data, in addition to our own clients. The prevalence and distribution of vulnerable Confluence instances at the time of disclosure are shown in the map below.



Atlassian released a fix on June 3. After the Confluence fix was announced, about 30% of vulnerable organizations patched within the first 10 days. However, the patch rate plateaued the following week without any meaningful rise the following week. This means that in practice 70% of vulnerable Confluence instances remained exposed beyond the average time to exploitation, representing a major risk for those organizations.

Confluence General Patch Trends in First 10 Days of Availability



Comparatively, the patching rate for organizations under observation that were informed by BlueVoyant's remediation services were significantly higher (60% patching rate at the 10 day mark) than those observed in general.

2. Zoho ManageEngine - Multiple Products Remote Code Execution Vulnerability CVE-2022047966

In many cases EV response rates are even less straightforward. In the case of the Zoho ManageEngine vulnerability, there were different moments of disclosure for vulnerabilities found within Zoho's ManageEngine products. Starting on October 27, 2022, Zoho began patching its ManageEngine products for the vulnerability tracked as CVE-2022-47966.[5] BlueVoyant observed a generally low patching trend in the first weeks following the disclosure, with the average percentage of patched instances being even lower than those of the Confluence vulnerability at the same comparable times.

Then, in late January 2023, security researchers released a proof of concept exploit code for the ManageEngine vulnerability that allowed for a remote code execution. The result was a notable uptick in patching trends starting on January 18, immediately following the disclosure of the POC exploit.

Through its data, BlueVoyant was able to detect this uptick and observe the change in the patching cadences for the four ManageEngine instances shown below:

BlueVoyant follows emerging vulnerabilities as they are released, and provided continuous updates as Zoho ManageEngine details were released. As in the case of the Atlassian Confluence vulnerability, organizations under observation that were informed by BlueVoyant's remediation services had significantly higher patching rates than those observed in public.

Takeaways and Recommendations

Despite the critical threat posed by emerging vulnerabilities, the overall trend of patching cadences across all industries for any given EV remains remarkably low. The issue around EVs highlights one of the key challenges that enterprise organizations face with regard to third-party cyber risk management today — it is difficult to get vendors to rapidly remediate vulnerabilities or high-risk behaviors, even if they represent a critical threat to organizations' extended IT ecosystem.

To counteract the threat of emerging vulnerabilities, which can become a critical attack vector quickly and without warning, there are a few best practices to take into account. It is important to maintain awareness of your internal services and technologies, as well as those of your supply chain. Maintaining a clear view of the services, technologies and products that you use allows you to assist and also make thoughtful decisions about how to engage with those services, including what data to share, etc.

It is important to be aware of your sector and what affects your business processes, not only for understanding sector-specific operational dependency but also in being threat-informed. Best practices will depend largely on what sector your organization operates in.

For example, if the nature of your infrastructure is to be open and accessible to a large number of users, such as in an academic organization, ensure greater consideration to user access and service dependencies. If you are in a sector dependent on industrial control systems, you must put extra consideration to the software versions you are running and patching. Critical service sectors have a larger stake in making sure that third-party vulnerabilities do not affect them since those third parties may not have the same oversight that primary organizations do in terms of compliance and regulation.

To specifically tackle the threat of EVs, it is critical to be able to quickly identify what the implications of a given vulnerability in your ecosystem is, in order to be able to address it in time. Ultimately, timeliness is the most important factor for zero-day vulnerabilities — when one is disclosed publicly it begins a race against time against attackers who will be actively searching for vulnerable instances. Your organization must aim to be able to patch vulnerabilities within the average time to exploitation, i.e. the time it takes attackers to take advantage of open vulnerabilities, which continues to decrease with each passing year.

BlueVoyant alerts clients within hours of a new vulnerability being disclosed, and works directly with third parties in order to improve the patching response times within the supply chain, who in many cases are not aware of the presence of the vulnerability.

Conclusion

Key Overall Takeaways

The trends outlined in this report highlight areas that organizations should focus on and dedicate resources to in order to implement an effective external cyber defense program. Notably, each of these issues pertain to organizations spanning across diverse sectors and geographies. While each threat actor, attack vector, and targeted organization may be unique, in general, the tactics and processes used by threat actors will tend to be similar across the board. Organizations looking to defend their assets can use this to their advantage and enhance their cyber security program and posture, as a targeted and efficient distribution of security-focused resources on the most common attack vectors laid out above can greatly improve their security posture at relatively minimal cost.

Several general takeaways and recommendations based on these trends have been provided by the security expertise at BlueVoyant:

- **Be proactive in tracking threats.** It is challenging to stay ahead of threat actors, but organizations should strive to stay well informed on current threat actor trends. This includes activities such as deep and dark web monitoring. From the examples above this is the only way to counteract emerging techniques such as the use of mule accounts.
- **Timeliness is key to capturing rapidly evolving threats.** Compliance policies and Regulatory guidance is not updated quickly. As threats emerge, especially when considering vectors such as emerging vulnerabilities it is unlikely that policies will keep pace. EVs can be disclosed and subsequently targeted and exploited within a matter of a few days or weeks, which usually outpaces organizational patching. Unfortunately, most risk mitigation practices focused on compliance or regulation are delayed in their ability to identify, let alone remediate vulnerabilities.
- **Look to the future in developing an agile security process.** Compliance and regulation provides good guardrails for critical industries, but it is important to take action before compliance standards make it a requirement. In addition to generally increasing your security posture this will allow an organization to avoid playing "catch up" to policies and regulatory standards that are often formalized months or years after attacker trends become common practice.
- **Be aware of your external ecosystem.** It is important to have full visibility of your external ecosystem's risk and your web presence, which includes all the processes, products, and services you are hosting. At minimum, an organization's security operations should frequently assess the entire external attack surface and web presence.
- **Prioritize risks and plan for the worst.** In addition to having awareness and visibility, it is important to be sure that even if your organization has risk, the potential damage inflicted by a cyber incident is the minimum damage possible. This concept relates to or includes direct business outcomes, operations, services, vendor and supplier dependency persistence, and general continuity of operation for all functions external to a company and its third-party ecosystem.

If organizations want to truly protect themselves against the myriad cyber threats that make up the modern attack landscape, they must be able to widen their security aperture to address the real threats from an extended ecosystem. The trends outlined above highlight the more prominent examples of threats to extended digital ecosystems, but it is clearly not an exhaustive list. It is our hope that as these issues becomes more widely recognized, that organizations will take more confident steps towards proactively and expediently improving their external cyber defense.

Endnotes

1 https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-040a

2 https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html

3 https://www.cisa.gov/news-events/alerts/2022/06/02/atlassian-releases-security-advisory-confluence-server-and-data

4 https://confluence.atlassian.com/confeval/confluence-evaluator-resources/confluence-features-functions

5 https://nvd.nist.gov/vuln/detail/CVE-2022-47966