Bitdefender

WHITEPAPER Jan 2023

Bitdefender MDR Insights: A 2022 Threat Assessment - and What's Ahead in 2023

Contents

2022 Threat Landscape

The year 2022 saw a continuation of the usual trends around vulnerabilities and the type of cyber attacks that have become prevalent over the past decade. We saw ransomware and criminal activity ebb and flow, as well as the use of offensive cyber operations during the war in Ukraine. Adversaries continue to use chains of exploits when attempting to gain access, while data exfiltration and intimidation continue to be the main goals.

2022 Vulnerabilities

In 2022, some of the most significant vulnerability exploits affected Microsoft and application layer platforms.

In May, CVE-2022-30190 threatened remote code execution (RCE) via the Microsoft Support Diagnostic Tool (MSDT). Widely known as "Follina," this critical vulnerability opened the possibility for an attacker to run code with system privileges, often through the abuse of all versions of legitimate, benign Windows applications.

Java-based Spring Framework had its share of vulnerabilities in March. It kicked off with Spring Expression denial of service (CVE-2022-22950), making it possible for a user to provide SpEL expressions that caused DoS conditions. Within one week, Spring Cloud RCE (CVE-2022-22963), functioning similarly to its predecessor, and Spring4Shell (CVE-2022-22965) were announced. Spring4Shell, a zero-day more widely publicized, was a remote code execution (RCE) in the Java-based Spring Framework.

Continuing with RCE vulnerabilities, Log4j (CVE-2021-44228) aftershocks continued to occur in 2022. In October, IBM announced that QRadar, IBM's SIEM, was affected by arbitrary code execution. Furthermore, cybersecurity researchers reported multiple campaigns and threat groups exploiting the Apache vulnerability, including a Linux botnet that communicated via DNS tunneling, APT41 targeting US state networks, and attacks against SolarWinds Serv-U.

We saw a continuation of exploits dubbed ProxyShell at the beginning of 2022 in the form of CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207 that affected access control, PowerShell, and allowed RCE in Exchange environments. Problems with Exchange grew into another issue that allowed an exploit called ProxyNotShell, which was associated with CVE-2022-41040 and CVE-2022-41082, affecting various versions of Outlook and Exchange services by allowing RCE, among other problems. Despite Microsoft issuing patches for these out-of-band and regular Patch Tuesday releases, many organizations did not apply patches promptly, falling prey to attackers who did not apply patches promptly.

Russia-Ukraine Conflict

In February 2022, during the initial phases of the Russian invasion of Ukraine, we offered some assessments about the then-developing situation to address possible customer questions and concerns. Back then, the best recommendation we had was to examine the situation through the lens of threat modeling, considering how and what the type of business a customer conducts and with whom might present an opportunity for a Russian-aligned adversary. Almost a year later, the factors to consider still ring true, with some slight updates:

- Do you have US/EU government contracts, especially those that might benefit Ukraine or NATO and EU allies?
- Are you providing direct assistance to the government or armed forces of Ukraine or any EU/NATO countries?
- Are you associated with any businesses or governments currently involved in sanctions?
- Does your business have information that would be of high value to a motivated nation-state, such as wartime operational or contingency planning, technical military data, or similar sensitive defense information?
- Do you have any contracts or may be involved in projects involving the Ukrainian
- government or companies, or have access to operational data as described above?
- Do you control financial services or assets that, if targeted by Russia, could impact the US or EU governments or the situation in Ukraine?
- Do you control or provide services to the Energy or IT Sectors, or businesses related to critical national infrastructure which could relate to the Ukrainian conflict?
- Are you actively part of a humanitarian assistance organization or operation, involved in the resettlement of displaced people, or otherwise directly assisting the people or government of Ukraine? This doesn't mean donations to the cause; this would imply being directly involved in boots-on-ground assistance to refugees.

During 2022 there were more interesting developments and revelations relating to cyber warfare in Ukraine, some of which warrant relooking military cyber operations; however, some disagreement remains over the effectiveness of Russia's use of cyberspace to advance its tactical and strategic military and political objectives. There was evidence of various malware deployed to attack Ukraine in the beginning and some isolated cases since. In addition to the malware, Microsoft reported on cyber operations occurring in support of kinetic, physical strikes by Russian forces. We also saw limited reporting on attacks on US and European organizations attributed to Russian actors. While Russian offensive cyber capabilities did not seem to play as big of a part as some experts initially predicted, that doesn't mean we will not see an increase in cyber operations or changes in operational tactics.

To err on the safe side, do not underestimate Russia's capabilities in this arena, despite some public missteps indicating some apparent mismanagement or misuse of resources. For years, Russian-aligned threat actors have shown high proficiency and capabilities with system tools and custom malware development, as well as the resources necessary to stand up various infrastructures in support of likely global operations. We know about some of the public failures and "almosts" of Russian operations, but the successes are still very possible behind closed doors in many ways.

Examining threat models against possible factors that lead to targeting of your organization will result in a better understanding of any remaining threats from the ongoing conflict in Ukraine. So far, Russia has deployed minimal attacks that we know of involving Ukraine and close allies, such as Poland or Romania; and we have yet to see widespread, wormable attacks similar to NotPetya that spilled over to Russia, in addition to their Ukrainian counterparts. CISA, Microsoft, and many leading cybersecurity and IT organizations have regularly released updates and research about the ongoing conflict, despite the situation recently falling out of high priority in news cycles compared to last year.

2023 Threat Landscape Predictions

Predictions are tricky, so we'll discuss the most likely threats and areas to consider based on observed threats in recent years. A few threats should be no surprise: Ransomware and phishing will continue to threaten everyone because both have relatively low barriers to entry and offer incredible returns on investment. In addition to those continuing trends, expect some of the following:

- We'll all continue seeing how remote and hybrid working environments impact threat models as more of the workforce demands more flexibility. This impacts how and where data is accessed and how secure the connections may be. Remote workers could be targeted for access, as we've seen in previous breaches of corporate Slack instances, or fooled by fake authenticator notifications that used elements of phishing.
- Supply chain attacks continue to showcase potential weak points in threat models and security planning. As we've seen in previous attacks, a determined and skilled adversary can inject themselves into software development or delivery processes or find other ways into a third-party organization.
- As a best practice, security should be included throughout the development cycle, rather than seen as an afterthought or expense.

Ransomware continues to contribute to cybersecurity woes in almost every industry, on almost every continent. While the attacks didn't seem to be on the same scale in terms of damage and media coverage this year, we did see the return of one big ransomware player, REvil, and the disappearance of another, Conti. The group names disappear, but the people behind the actors often move to other groups or start new ones. At this point, the biggest lesson learned from ransomware is that no one is immune from these attacks, as we've seen a fair share of governments, cybersecurity vendors, and managed service providers alike fall victim, as well as companies big and small. The most common themes among ransomware victims are that they're service providers based in North America or Europe, so if your company falls into that category, you're already at risk.

Another area to consider that was brought up by our colleagues at ZeroFox in their 2023 forecast is the implications of adopting and developing new technologies. In just the last few years, we have seen huge jumps in capabilities around artificial intelligence, more frequent and widespread transactions with nonphysical assets such as non-fungible tokens and cryptocurrency, increased processing power, and lower costs of technology that comes with cloud-based applications, services, and storage. While beneficial in many ways to consumers and businesses, all of this presents new attack surfaces and opportunities for adversaries; the effects of which are still being discovered and understood.

Inside MDR Operations in 2022

MDR Incidents

The goal of the Bitdefender MDR SOC is to catch attackers as far left of the attacker's life cycle as possible. A common theme seen by our SOC was unmonitored hosts becoming the launching point of a security incident. Unmonitored hosts, usually deemed less critical, can still pose a severe threat to monitored environments and allow attackers to go undetected during initial access and further as they move through the other steps, like persistence or privilege escalation. In addition, attackers took advantage of critical vulnerabilities involving Log4j and ProxyShell, a Microsoft Exchange vulnerability, using various web shells to conduct reconnaissance, create new user accounts, and download additional malware on the infected systems.

To help reduce the risk of these threats, here are recommendations for all MDR customers:

- Regular patch management and auditing of accounts and tools can help reduce the risk of these threats.
- Use attack surface tools to discover gaps in security tool coverage
- Add Bitdefender XDR, which provides better observability into endpoints, networks, identities, and cloud workloads
- Incident response policies – Ensure policies are in place to detect and triage security incidents. If using an MDR service, those incident response policies should include how to communicate and use those services to reduce the business impact

Intelligence Alerting and Monitoring Trends

Domains on Code Repositories

The Cyber Intelligence Fusion Cell (CIFC) alerts have been steady throughout the year. Analysis shows that the most triggered alert type is Domains on Code Repositories. It's important to remember that code and data stored on code repositories and paste sites should be privatized and audited often, especially as people move on and projects end. Bottom line: if you have developers on staff, you should look into having private Git instances set up that don't publicly expose internal project data and code. If there are public instances needed for scholarly reasons or collaboration with third parties or the public, these instances should be audited to ensure they're still needed and not exposing any critical information.

Typosquatting

The second most triggered alert type from CIFC – as well as the second highest communication to customers – concerns typosquatting. Typosquatting and similar activities have increased significantly within MDR-monitored assets compared to last year (Figure 1 below) – most notably from November to December 2022. Should a customer be notified of this activity, the best course of action is to have malicious domains taken down with the registrar, block the domains, and make users aware of potentially suspicious or malicious domain activity.

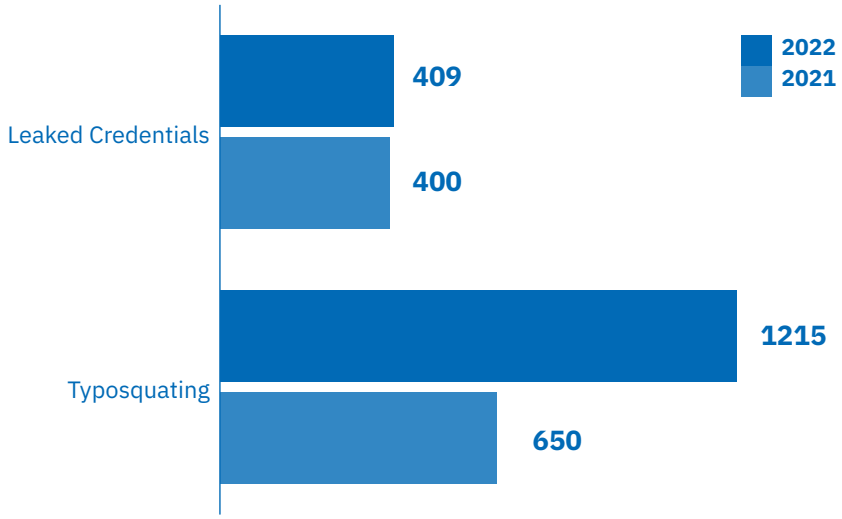

Figure 1: MDR CIFC typosquatting and leaked credential alert comparison

This year, researchers reported massive phishing and typosquatting campaigns that occurred globally. One campaign, discovered by Bleeping Computer and Cyble, targeted Windows and Android users with over 600 domains and 27 brands in their arsenal. Another bit of concerning research showed domain registrations related to Facebook, WhatsApp, and Instagram with various types of malicious intent, including spam, hacking, and credential theft. Users of well-known banks, payment services such as PayPal or Coinbase, and e-commerce such as Amazon, iTunes, and similar brands are constantly targeted. Phishing has increased since the beginning of the pandemic and migration to remote and hybrid working. Spanning reported that an estimated 90% of cyberattacks are phishing, but an even scarier statistic disclosed by Swiss Cyber Insititute was that 1.5 million new phishing websites are made monthly. This is a major pain point for our customers, as seen in the number of requests for information submitted to CIFC. It's important to note that phishing targets every industry and individual; therefore, users should take preventative measures and be careful what they click.

CIFC recommends that customers should regularly audit domains to ensure that purchased domains still have a purpose or are otherwise still fulfilling a business need, and shutting down those domains that are no longer relevant or necessary.

Leaked Credentials

The top customer notifications are for leaked credentials. Credential leak activity stayed proportionate to last year's trends (Figure 1 above). One of our credential monitoring highlights this year is the addition of a source called Malware Logs (see Appendix). To mitigate risk, customers should limit access to business systems to only monitored environments that meet the company's security requirements. Educate users about using their business emails on third-party websites; however, if the use of company email on outside sources is necessary, make sure users are creating different and unique passwords or, better yet, using a password manager.

MITRE Enginuity ATT&CK Evaluation for MDR

MITRE, an internationally recognized organization known for the ATT&CK framework, released its first Engenuity ATT&CK® Evaluation for Managed Services results on November 9, 2022. The evaluations serve as an impartial starting point to understand how managed security providers identify attacks and what is delivered by the participants.

Our globally distributed teams treated this as a real incident during the weeklong exercise. As one of our guiding principles, Bitdefender MDR operated as closely as possible to our standard procedures. The Bitdefender Labs organization worked with our SOC analysts, investigating detections and attacker techniques, while CIFC provided additional context behind observed behaviors and potential investigational pivots to assist SOC hunts. The Bitdefender MDR team leveraged our native security stack to detect 100% of the attack steps while providing actionable, summarized output with a clear timeline of the attack and recommended actions. The SOC used existing reporting mechanisms to deliver daily updates and post-incident reporting, just as we do in real-world incidents. Bitdefender MDR capitalized on lessons learned and continually strives to identify opportunities to improve our incident handling processes that ultimately improve our service for our customers. See more about Bitdefender MDR's performance in the Bitdefender November Threat Debrief.

Bitdefender Results

Bitdefender Threat Debrief

In May 2022, CIFC was asked to collaborate with the Labs organization – Bitdefender engineering and research experts known for working with European law enforcement agencies and creating decryption tools for ransomware such as REvil/Sodinokibi, MamoCrypt, and MegaCortex – on one of Bitdefender's monthly blogs. The Bitdefender Threat Debrief, first released in August of 2021, is an article providing threat data trends and intelligence observations on the latest threat news and operational highlights. MDR Insights has become a valuable addition to the Threat Debrief, captivating readers' attention more and more each month, along with noteworthy mentions by CIOMX in Mexico and BPS Business Publications and Silicone in Spain. CIFC has focused on compelling topics, deep-diving into threat modeling, intelligence monitoring activity, and our take on current exploits. This could lead to a separate spinoff product specifically for our MDR customers, but until then, be sure to check out Bitdefender's Business Insights each month!

Conclusion

Threats are everywhere, but defenses-in-depth that consist of everything from user training and XDR solutions to tools and access and vulnerability management can help mitigate the daily risks every organization faces to stay connected to the internet. Besides the one-off and emerging threats, there are near-constant threats. CIFC recommends maintaining vigilance against social engineering, which includes phishing with weaponized attachments or compromised URLs. Ensuring that there are backups available and keeping infrastructure patched, help keep adversaries who exploit vulnerabilities or employ ransomware techniques at bay and offers a degree of risk mitigation.

Again, we cannot stress enough how effective vulnerability and patch management programs can reduce risks from multiple adversary types. While zero-days and custom malware are scary, the path and turnaround time from announced vulnerability or proof-of-concept to exploit is getting shorter every year. Understanding the cost-benefits and risks of hosting on-premises or running applications in-house versus the cloud go hand-in-hand with vulnerability and attack surface management, and should also be considered.

Lastly, It's important for security teams to understand the evolving tactics of myriad emerging threats, as well as knowing the baseline to search for the anomalies and indicators; but much of this also depends on how open an environment is to attackers and how well a customer knows their own network.

Organizations are attacked every day around the world, and often the initial vector was the result of an old, or well-known vulnerability that was exploited by automation, or caused by inattention. Many cloud providers manage the infrastructure, which creates more capacity for in-house support teams to tackle other technical debt or more pressing issues. The capabilities to monitor these areas are growing and being adopted by more vendors, which is probably the next security frontier in a post-XDR world.

Appendix

CIFC Monitoring Details

Domains on code repositories – Code repositories and paste sites, such as GitHub and PasteBin, are monitored for domain and brand name mentions due to their easy public access. It is not uncommon for threat actors, as part of their reconnaissance, to monitor these sites for information on their targets, such as proprietary code and data, the names or emails of people working on a project, or cloud access keys.

- Adversaries may also store their own information about their targets on code repositories, often anonymously.

Typosquatting – Threat intelligence tooling is catching everything from domain and certificate registries and changes, to subdomains that are identified during scanning, which are oftentimes either unrelated activity or the domain is still for sale.

- The most common way that threat actors use typosquatting is to impersonate specific domains and brands in an attempt to lend credibility and appear benign through a variety of methods.

Leaked Credentials – Threat intelligence tooling provides access to credential leak sources, but not all of them or in a timely fashion. It is very likely there are breaches and exposures the security world at large does not know about yet, so proactive access management is needed because relying on third parties for breach information might be too late.

- Malware Logs – Malware Logs contain data from various information-stealing malware that gathers browser information (primarily credentials) from individual computers. A source such as this has a higher criticality because, unlike combination lists or old breach information, this source represents fresh, stolen credentials typically in use within the last 30 days. Since there's a good chance these passwords are still in use somewhere else, CIFC notifies customers as soon as possible.

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com