CyberTalk.org

FIVE DANGEROUS CYBERATTACKS

YOU SHOULD EXPECT IN 2023

Cybercrime is big business, and it has proved to be extremely profitable for threat actors. Sophisticated criminal syndicates are taking cues from Fortune 500 companies — implementing strict hierarches, payroll, HR, and more.

In 2022, the world has witnessed defining events across the cyber landscape, from the Russia-Ukraine war and state-sponsored attacks to Conti's ransomware attacks on the countries of Costa Ria and Peru — not to mention a myriad of multi-million-dollar scams in crypto.

What can we expect looking forward?

In this report, you will discover five dangerous cyberattacks that have largely gone under the radar but have the potential to wreak massive havoc on any organization. In addition, you will learn why traditional methods of cyber security are no longer effective – and what you can do to improve your cyber security posture in 2023.

> "Global cybercrime damage is predicted to hit $10.5 trillion annually by 2025."
>
> — Steve Morgan, Cybersecurity Ventures

Country-level extortion attacks

When ransomware was first introduced, it was mainly individuals or small groups who conducted ransomware operations, distributing ransom emails to collect small amounts of ransom from individuals. Over the years, hackers realized how lucrative it is to target large corporations that have revenues in the hundreds of millions and sometimes billions of dollars, as they can afford to pay larger sums of money.

Now, hackers are picking fights with entire countries. For example, the Conti ransomware group extorted the countries of Costa Rica and Peru, and Lapsus$ also began attacking governmental entities. With a scale of operations that involves research and development, quality assurance, HR, and physical offices – ransomware gangs can now take on any entity, no matter the size.

Large ransomware groups, however, have an inherent vulnerability: it becomes more difficult to stay under the radar. It's hard to conceal a multi-million dollar business that employs hundreds of skilled workers with offices in major cities. The larger the business, the more it becomes dependent on the cooperation or at least passive acceptance from the government in which it resides. As a result, groups are forced to align with the geopolitical interests of their home countries.

For example, Russian authorities arrested members of the REvil ransomware gang in January 2022.[1] However, the group's blog and Tor network resumed to full activity by April, strangely coinciding with the war in Ukraine – suggesting that Russia is potentially using REvil for its own political agendas.

In April 2022, Conti attempted to extort the entire country of Peru. Conti successfully infiltrated the country and extorted two key government entities – the Ministry of Finance and General Intelligence Directorate. On May 7th, Conti successfully breached Peru's national intelligence agency and stole 9.5 GB of sensitive data.

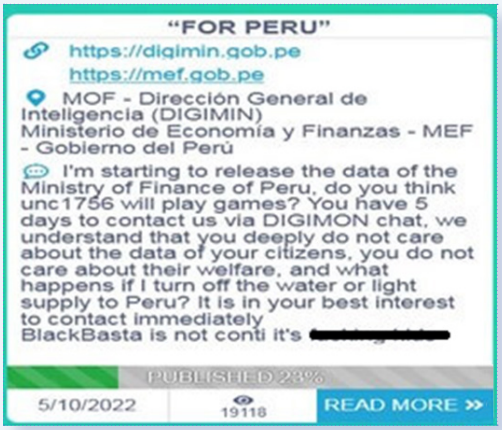

Figure 1: *Conti's extortion message to Peru after pilfering data from: " Country Extortion: Ransomware expands business to include the government sector," Check Point Software, https://blog.checkpoint.com/2022/05/26/country-extortion-ransomware-expands-business-to-the-governmental-sector/*

In parallel, on May 12th, Costa Rica's president declared a state of national emergency and announced that the country was at war with Conti, which is the first time that a country ever declared war on a cybercrime group. This took place days after Conti breached and encrypted data from at least 27 Costa Rican governmental agencies.

Leaders of countries often talk about investing in infrastructure. However, in addition to physical infrastructure, countries must also invest in their cyber security infrastructure if they want to avoid becoming the next victim of a cyberattack and suffering drastic consequences.

Cloud supply chain attacks

As many as 98 percent of companies use[2] cloud-based services, and 76 percent of them have multi-cloud environments, utilizing services from two or more cloud providers .[3] When organizations move to the cloud, this increases their reliance on third parties and partners, which can exacerbate the risk of threats throughout the supply chain.

---

[1] "2022 Mid-Year Trends Report," *Check Point Software*, 4 Aug. 2022, https://pages.checkpoint.com/cyber-attack-2022-trends.html.

[2] "The Biggest Cloud Security Challenges in 2022 | Check Point Software," *Check Point Software*, 18 Apr. 2022, https://blog.checkpoint.com/2022/04/18/the-biggest-cloud-security-challenges-in-2022-check-point-software/.

[3] Ibid.

> Eighty-one percent of organizations are moderately to highly concerned about risks surrounding suppliers and partners.[4]

Supply chain attacks became mainstream in the past few years, from the SolarWinds Orion software breach – an innovative on-premise-to-cloud incident in which hackers leveraged a backdoor to gain access into private cloud environments – to the Log4Shell vulnerability, a bug that allowed threat actors to gain control over Java-based web servers and execute malicious code.

Supply chain attacks are about to meet the cloud arena. On March 21st in 2022, ransomware group Lapsus$ achieved access to Okta, an identity management platform, gaining access to its customers. Okta is responsible for securing user authentication processes as well as building identity controls, which means that hundreds of thousands of users were potentially compromised by the company responsible for their security.

Check Point Research (CPR) suggested[5] that Lapsus$'s impressive record of successes could be due to its breach of Okta.

Although the Okta breach is not necessarily a cloud supply chain attack, which would occur if a provider such as Azure or AWS were compromised, it was a significant cyber incident that affected the supply chain and alerted businesses to be more cautious regarding Identity and Access Management (IAM) role abuse attacks. According to CPR, the most prominent supply chain risk is coming from open-source software, which makes sense because individuals who write open-source code may not have the expertise or budget to make it completely secure.

When it comes to your chosen cloud provider, such as AWS or Azure, you cannot control how the platforms conduct its security. However, you should have multiple layers of security, so that if a cloud provider ever does get breached, you are able to mitigate the fallout. Implementing zero-trust and least privilege access can also help contain and stop the spread of an attack.

---

[4] Plumb, Taryn. "Cloud security: Increased concern about risks from partners, suppliers," Venture Beat, 19 Aug. 2022.

[5] "LAPSUS$ & OKTA: The Cyber Attacks Continue," *Check Point Software*, 22 Mar. 2022, https://blog.checkpoint.com/2022/03/22/lapsuss-okta-the-cyber-attacks-continue/.

Developments in email infection chains

Did you know that 34 percent of burglars break into homes through the front door? They simply twist the knob and walk right in. Likewise, in the cyber realm, Microsoft Office documents act as our digital front doors. Everyone uses them without worrying about the security implications, which is exactly what makes the Office document such an attractive attack vector to hackers. Malicious documents, or maldocs, involve the abuse of Office Macros, which are a highly versatile tool with extensive programming capabilities.

To combat this, in February 2022, Microsoft announced[6] it would change Office's default settings to disable macros. As stated on Microsoft's page,[7] macros are often used for malicious purposes:

"Macros automate frequently used tasks to save time... Many were created by using Visual Basic for Applications (VBA) and are written by software developers. However, macros can pose a potential security risk. Macros are often used by people with malicious intent to quietly install malware, such as a virus, on your computer or into your organization's network."

Exploits using VBA macros appeared as early as 1995. However, they did not have the information-stealing functionality that macros have today and were mostly used for pranks. Macro attacks dwindled in 2010 when Microsoft introduced "Protected view," which is a yellow ribbon that warned users not to enable macros. However, threat actors maneuvered this with a bit of social engineering. They would simply convince users to enable macros, resulting in the macro downloading and executing other binaries.

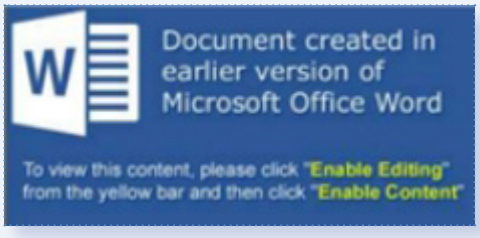

Figure 2: *Typical label designed to convince the victim to enable macros from: "2022 Mid-Year Trends Report," Check Point Software, pages.checkpoint.com/cyber-attack-2022-trends.html*

Throughout the years, the use of Office macros and vulnerabilities increased in popularity. By January 2022, Check Point Research discovered[8] that 61 percent of all malicious payloads attached to emails were various document types (xls, doc, pdf, etc.). Excel files make up 49 percent of all malicious files received via email. For non-sophisticated actors as well as APTs, a carefully socially engineered email carrying an Excel file with a malicious macro is their weapon of choice.

---

[6] Eickmeyer, Kellie. "Helping users stay safe: Blocking internet macros by default in Office," *Microsoft*, 7 Feb. 2022. https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/ba-p/3071805

[7] "Enable of disable macros in Office files," *Microsoft.* https://support.microsoft.com/en-us/office/enable-or-disable-macros-in-office-files-12b036fd-d140-4e74-b45e-16fed1a7e5c6

[8] "Mid-Year Trends Report 2022" (n 1).

Figure 3: *Percentage of Excel files of the total malicious files received by email from: "2022 Mid-Year Trends Report," Check Point Software, pages.checkpoint.com/cyber-attack-2022-trends.html*

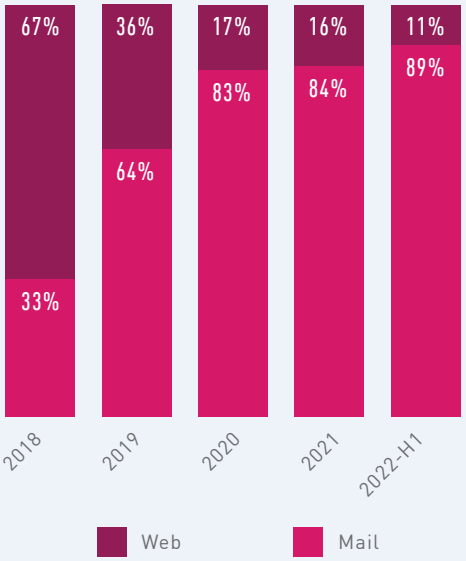

Figure 4: *Increase in proportion of malicious files sent by email from: "2022 Mid-Year Trends Report," Check Point Software, pages.checkpoint.com/cyber-attack-2022-trends.html*

However, the decision to disable macros forced threat actors to innovate and develop new infection chains, with different file types than just regular Office files. For example, Emotet[9] was reported in April to be testing new TTPs (Tactics, Techniques, and Procedures), emailing OneDrive URL links of zip files containing malicious .xll files, which are .dll libraries designed for Excel.

Threat actors may also use ISO archives, which bypass the MOTW mechanism. They look like documents, while running malware in the background. In addition, hackers may password protect their documents to bypass further malware detections. HTML template injections are another example of a Microsoft Office exploit, as seen in Follina, a word document that uses a remote template feature to retrieve an HTML file before executing a PowerShell.

In conclusion, the best defense is for users to become aware of sophisticated social engineering. Cybercriminals will often send a simple email impersonating someone to get into conversation with you and gain your trust before sending you a malicious file. Consider implementing a Security Awareness Training program to equip your employees with the skills they need to spot the red flags in a phishing attempt.

[9] "Mid-Year Trends Report 2022" (n 1).

The new era of hacktivism

Hacktivism is no longer reserved for decentralized collectives that consist of individuals with a variety of agendas. Hacktivism is now well-organized, structured, and more sophisticated – and these groups often adopt the agenda of the country in which they reside.

Figure 5: *Example of contradictory campaigns launched by Anonymous from: "The New Era of Hacktivism," Check Point Software, https://research.checkpoint.com/2022/the-new-era-of-hacktivism/*

Major hacktivist groups that appeared in the past couple of years also share the same characters that a structured organization has: a clear and consistent political ideology, a well-structured hierarchy for employees and leadership, and a formal recruitment process. These groups sometimes cooperate with each other and have public relations operations to publicize their successes across major media channels, websites, and forums. All this allows governments to mobilize these hacktivism groups to align with their political agendas and achieve broad-based goals that have wider public impact than ever before.

The shift in hacktivism[10] began around two years ago in the Middle East, with several hacktivist groups – such as Hackers of Savior, Black Shadow, and Moses Staff – focusing their attacks exclusively on Israel. Many of these attacks publicly promoted their affiliation with the Iranian regime. In parallel, other groups in the Middle East solely attacked pro-Iranian targets.

However, hacktivism was not only limited to the Middle East but also extended to the Russian-Ukrainian war. In the beginning of 2022, an anti-Belarussian cyber group began launching destructive cyberattacks to hinder Russia's troops. Ukraine's IT Army was also mobilized to attack Russia. Anyone that opposed either Russia or Ukraine also became potential targets from the other side, broadening the sphere of impact.

[10] "The New Era of Hacktivism – State-Mobilized Hacktivism Proliferates to the West and Beyond," *Check Point Research*, 29 Sep. 2022, https://research.checkpoint.com/2022/the-new-era-of-hacktivism/

Governments in Europe and the US have also fallen victim to this emerging type of hacktivism from state-mobilized groups. For example, the Albanian government fell prey[11] to hackers connected with the Iranian military. Corporations such as Lockheed Martin, a global defense contractor, have suffered severe attacks stemming from these groups as well.

In summary, the rise of hacktivist groups is not expected to slow down anytime soon. Government agencies and private organizations should consider themselves duly warned and begin improving their cyber security infrastructures, whether they reside in a country involved in an ongoing political conflict or not.

First attacks in the metaverse

The metaverse is a hot topic. It promises an escape from reality through a headset that beams a 3D virtual reality to the user. It allows you to live a rich digital life in which you can spend time together with friends, shop for real or virtual items, play games, and more. However, with all the discussion surrounding the metaverse, one issue is often overlooked: cyber security.

> 25% of people are expected to spend at least an hour a day in the metaverse by 2026—but this opens them up to a myriad of crimes.[12]

The Metaverse is built on the blockchain, so it should not be long before we start to see initial attacks in the Metaverse too. According to Check Point Research, these attacks will be based on authorization and user accounts will get hijacked.

Furthermore, a new report[13] from Europol Innovation Lab urges police forces to start thinking about the security challenges brought on by the metaverse.

The Europol report warns of the following threats related to the Metaverse:

- Ransomware targeting devices such as VR headsets
- Identity theft and fraud

[11] Powell, Olivia. "Albanian government falls prey to 'unprecedented and dangerous' cyberattack," *Cybersecurity Hub*, 20 Jul. 2022, https://www.cshub.com/attacks/news/albanian-government-falls-prey-to-unprecedented-and-dangerous-cyberattack

[12] Collard, Anna. "Crime in the metaverse is very real. But how do we police a world with no borders or bodies?" *WeForum*, 18 Aug. 2022. https://www.weforum.org/agenda/2022/08/crime-punishment-metaverse/

[13] Muncaster, Phil. "European Police Warn of Metaverse Cyber-Threats," *Infosecurity Group*, 24 Oct. 2022. https://www.infosecurity-magazine.com/news/european-police-warn-of-metaverse/

- Misinformation campaigns
- Harassment, child abuse, and exploitation
- Money laundering via cryptocurrencies as well as non-fungible tokens (NFTs)

For the metaverse to survive cyber security threats, it must adopt a zero trust model that requires strict identity checks, preventing bad actors from infiltrating networks. With such large amounts of data hosted in the metaverse, a zero trust model in combination with AI-driven cyber security tools will be an effective way of reducing the theft of sensitive information.

As the metaverse starts to evolve, the companies involved in creating it or any related products need to start building a more secure experience in its early iterations. By doing so, this will help reduce the number of security incidents as the metaverse grows.

Recommended cyber security practices in 2023

As your organization faces new and existing cyberattacks in 2023, consider implementing the following list of cyber security best practices:

- **Install updates and patches regularly.** WannaCry hit organizations around the world hard in May 2017, infecting over 200,000 computers in three days. However, a patch for the exploited EternalBlue vulnerability had been available for a whole month before the attack. Updates and patches must be installed immediately and on an automatic schedule.
- **Adopt a prevention-first strategy and approach.** A detection-only approach is not enough. Cyberattacks can be targeted and evasive, and if data is stolen, the costs to the organization will be high. Once an attack has penetrated a corporate network in any way, it is too late. It is therefore essential to use advanced threat prevention solutions that stop even the most advanced attacks as well as prevent zero-day and unknown threats.
- **Install anti-ransomware protection.** An anti-ransomware solution looks out for any unusual activity such as opening and encrypting large numbers of files, and if any suspicious behavior is detected, it can react immediately and prevent massive damage.
- **Implement a Security Awareness Training Program.** Many cyberattacks can start with a targeted email that does not contain malware but uses social engineering to try to lure the user into clicking on a dangerous URL. User education is therefore one of the most important parts of protection.
- **Collaborate with government entities.** In the fight against cybercrime, collaboration is key. Contact law enforcement and national cyber authorities; do not hesitate to contact the dedicated incident response team of a cyber security company. Inform employees of the incident, including instructions on how to proceed in the event of any suspicious behavior.

- **Beware of requests to sign links within any marketplace.** To prevent the theft of crypto keys and wallets, be careful whenever you receive a request to sign links within marketplaces. Prior to approving a request, review what is being requested and consider whether it seems abnormal or suspicious. If there are any doubts, you should reject it. Token approvals can be reviewed and revoked using this link: https://etherscan.io/tokenapprovalchecker

Conclusion

Cyberattacks are becoming incredibly complex. Hackers have developed cyberattacks to a scale that allows them to thwart entire nations. Against this backdrop, we are increasingly seeing threats having a disruptive physical impact in the real-world regarding geopolitical conflicts, as well as attacks that extend to the metaverse and the cloud supply chain.

While you cannot always predict when the next cyberattack will come, a layered and preventative approach to cyber security can mitigate most risks. For IT security teams, that means consistent training and drills; for your systems, frequent updates and continuous monitoring, often delivered through the cloud. Moving forward, A.I. will play a greater role in automating security, allowing security analysts to ignore mundane, rote tasks and focus on what they do best: preventing cyberattacks.

This report was made possible thanks to the cooperation of Check Point Research.
For more detailed information on the threats and trends discussed here, download the 2022 Mid-Year Trends Report.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391 / 650-628-2000

www.checkpoint.com