

Whitepaper

SANS 2023 Attack and Threat Report

Written by [John Pescatore](#) and [Terry Allan Hicks](#)

June 2023

Introduction

By now, most CEOs, boards of directors, and other high-level enterprise decision makers are well aware of the risks that cyber threats represent to the ongoing success of their business operations. They've evolved metrics and processes for evaluating the strategies that business unit managers, CIOs, and CFOs present to them. They can use these metrics to rank risks and opportunities, outline strategies, and create timeline projections of proactive plans for both meeting business goals and managing risks. Too often, however, CEOs and directors report that CISOs don't seem able to provide that same level of connection between security risks, business goals, and strategies (not tactics) to effectively and efficiently manage (not eliminate) risks. They report that CISOs are strong on identifying very scary risks, but weak on prioritizing risks and remediation strategies and developing and reporting on business-relevant security metrics.

The first step in overcoming these challenges and obtaining management support for changes needed to raise the cybersecurity bar is for CISOs and other security leaders to understand the rapidly evolving threat landscape and—crucially—its impact on enterprise risks.

For more than 15 years, the SANS Institute's "Five Most Dangerous Attacks" expert panel at the annual RSA Conference has provided the up-to-the-minute information on emerging cyber threats and their impacts that CISOs need. This SANS whitepaper builds on a baseline of statistics from proven sources of breach and malware data, and then goes deeper to detail the expert advice offered by the SANS instructors presenting at RSA Conference 2023—held in April—on the most dangerous emerging threats to look out for now and in the future.

2022/2023 Breach and Threat Baseline Data

We'll begin with a baseline from data collected by the Identity Theft Resource Center (ITRC),¹ a nonprofit organization that works to minimize the risk and mitigate the impacts of identity compromise. The ITRC has applied a consistent methodology for many years, using only verified information from publicly disclosed breaches. It doesn't include incidents, like denial-of-service attacks, that don't result in exposure of private information, but it does include most recent ransomware attacks. See Figure 1.

	2022	2021	2020
Cyberattacks	1,595	1,613	878
Phishing/Smishing/BEC	461	537	383
Ransomware	276	352	158
Malware	70	141	104
Non-Secured Cloud Environment	9	24	50
Credential Stuffing	18	14	17
Unpatched Software Flaw	-	4	3
Zero Attack Day	8	4	1
Other	26	426	162
Not Specified	727	111	-
System & Human Errors	151	179	152
Failure to Configure Cloud Security	18	54	57
Correspondence (Email/Letter)	55	66	55
Misconfigured Firewall	30	13	4
Lost Device or Document	6	12	5
Other	23	34	31
Not Specified	19	-	-
Physical Attacks	46	51	78
Document Theft	7	9	15
Device Theft	21	17	30
Improper Disposal	5	5	11
Skimming Device	6	1	5
Other	6	19	17
Not Specified	1	-	-
Data Leaks	-	7	-
Unknown	10	12	-
Totals	1,802	1,862	1,108

Figure 1. Security Compromises by Attack Vector
(Source: ITRC 2022 YE Data)

¹ "Notified," Identity Theft Resource Center, <https://notified.idtheftcenter.org/s/>

The ITRC data shows a slight decrease in the number of breaches reported in 2022, compared with 2021. The number of records exposed, however, rose dramatically, from 298,213,506 in 2021 to 422,143,312 in 2022, for an average of more than 234,000 records exposed per breach. The hard costs of a breach of that size typically are calculated to be in the \$100-per-record range, which means the average cost of a reported breach in 2022 was more than \$24 million.

One significant factor the ITRC notes is that 40% of breaches in 2022 were via supply chain partners. That is consistent with SANS Institute’s observations that as an enterprise raises its level of security maturity, its supply chain partners often become the weakest point in its defense. These aren’t the only third-party sources of security failures. We’ve also seen malicious actors focusing on service providers as a means of compromising multiple targets simultaneously.

The ITRC reports that a major trend in 2021 *and* 2022 has been fewer breach reports releasing detailed information indicating the root cause of the breach. This is likely due to recent court rulings requiring that actual damage, not potential harm, be proven in order for a damage claim to be upheld. This lack of information for 2022 reports makes direct comparisons with 2021 somewhat more difficult. However, looking only at breaches where root cause information is available makes some trends clear, including:

- Successful phishing attacks are still the leading cause of breaches at 53%, up from 36% in 2021.
- Ransomware was still a growth industry in 2022, up to 32% from 23% in 2021.
- Zero-day attacks still represent only a small fraction of root cause reports, at under 1%.

Just as this report was being finalized, the ITRC released statistics for Q1 2023. The overall numbers largely mirror Q1 2022’s, but the number of breaches and records exposed doubled for the technology sector. This is consistent with continued criminal focus on compromising service providers in technology. See Figure 2.

	Year					
	Q1 2023		Q1 2022		Q1 2021	
	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	31	357,001	21	106,099	24	112,684
Financial Services	70	1,707,880	68	5,732,597	49	7,848,115
Government	23	758,901	13	790,763	11	647,917
Healthcare	81	13,879,551	73	4,377,462	71	3,332,703
Hospitality	6	176,404	6	57,392	6	53,152
Manufacturing & Utilities	54	38,161,023	52	249,706	38	384,934
Non-Profit/NGO	18	75,222	20	629,822	15	509,219
Professional Services	42	69,227	45	3,022,491	30	3,566,213
Retail	16	170,080	18	272,950	20	506,821
Technology	33	22,362,858	16	10,832,588	23	17,377,396
Transportation	12	11,095,128	8	20,930	14	139,250
Other	59	327,411	64	675,411	53	6,695,075
Unknown	-	-	-	-	-	-
Totals:	445	89,140,686	404	26,768,211	354	41,254,479

Figure 2. Compromises by Sector: Q1 2023 vs. Q1 2022 and 2021

The annual Verizon Data Breach Investigation Report (DBIR), first released in 2008, has consistently been another rich source of information about attacks and threats. The DBIR is based on incident response investigations of actual successful attacks, so it provides the most detailed root cause information available (see Figure 3).

The single most important factor enabling successful attacks in 2022 was the attackers’ use of reusable credentials, mostly obtained with phishing techniques. Enhanced security awareness and education along with better email security gateways have reduced the percentage of phishing emails users click on. But when enterprises rely on reusable passwords, all it takes is one click on the wrong link and the game is over.

Verizon’s investigation found an even higher rate of supply chain compromise than the ITRC, reporting 62% of intrusions involved a supply chain partner. A key point from the DBIR: “Compromising the right partner is a force multiplier for threat actors. Unlike a financially motivated actor, nation-state threat actors may skip the breach and keep the access.”² This means that time-to-detect is key to minimizing damage from supply chain attacks that—as is often the case in politically motivated attacks—have the goal of monitoring an enterprise’s research-and-development (R&D) and business efforts over an extended period.

The DBIR did have some good news on the time-to-detect front, showing that enterprises are now more likely to detect in days rather than months. But, of course, this is only for the 50% of breaches not “actor disclosed,” as often happens in ransomware events. See Figure 4.

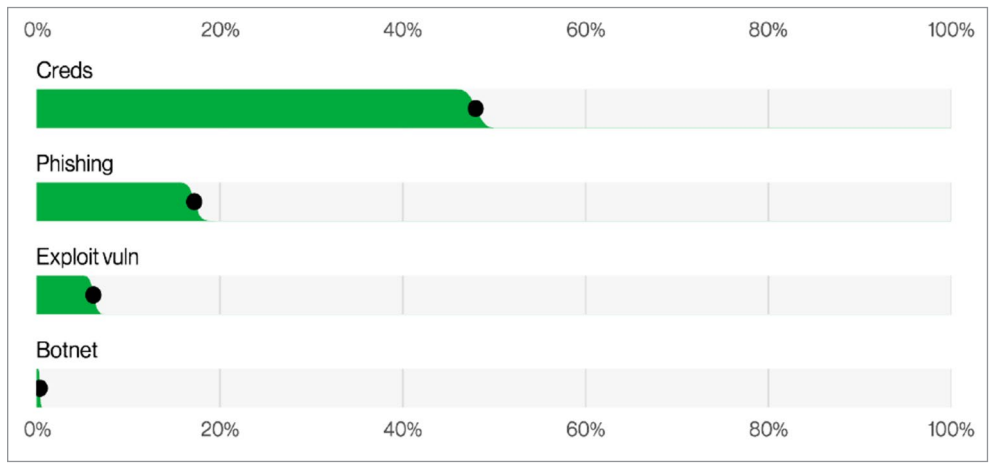


Figure 3. Leading Root Causes of Successful Attacks, 2022 (Source: Verizon DBIR)

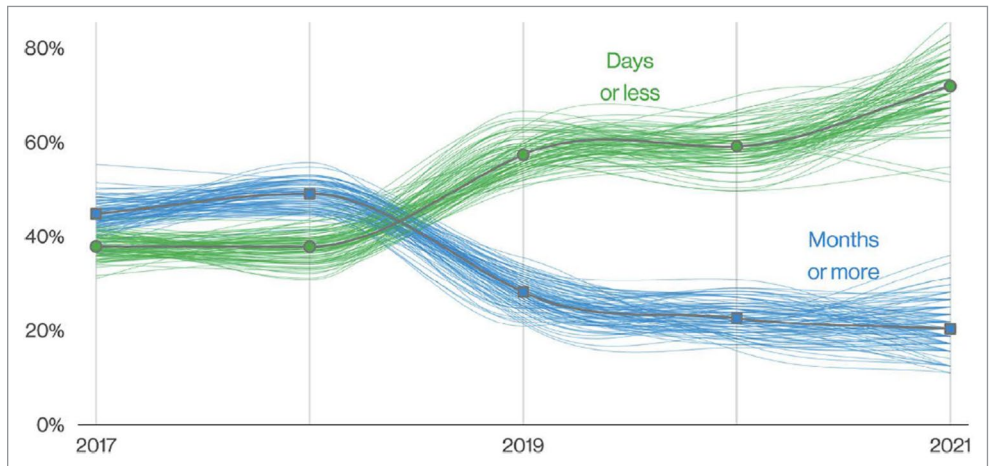


Figure 4. Detection in Non-Actor-Disclosed Breaches (Source: Verizon DBIR)

² “Verizon Data Breach Investigations Report 2022, Summary of Findings,” www.verizon.com/business/en-gb/resources/reports/dbir/2022/summary-of-findings/

What does all this data tell us about the current threat environment? Essentially, that although there have been definite improvements in some areas—notably end-user security awareness and endpoint protection—the bad actors are constantly evolving their tools and techniques. That means CISOs and other security leaders must be constantly updating their knowledge of the threat environment and the risk impacts of emerging threats on enterprise operations. The presentations by the expert panelists at RSA Conference 2023 are an excellent place to start. They included these takeaways:

- Reusable passwords remain irresistible low-hanging fruit for threat actors.
- Where enterprises have strengthened their levels of essential security hygiene, attackers are going after supply chain partners as the “screen window” access point.
- Zero-day attacks get the headlines, but 99% of breaches exploit well-known vulnerabilities in people, processes, and software for which mitigation actions are available and widely known.

Hear from the Experts: SANS Threat Panel at the RSA Conference

Since its inception in 1991, RSA Conference has grown into one of the world’s largest and most important cybersecurity conferences. For many years, one of the highlights of the event has been a panel where the SANS Institute’s top experts present their views of the most dangerous emerging attacks—attacks that are just beginning to impact enterprises. Time and again, the predictions by SANS instructors at these sessions have proven to be highly accurate predictors of real-world damage.

The 2023 threat panel was moderated by Ed Skoudis, president of the SANS Technology Institute. This year’s threat experts (shown in Figure 5) were:

- **Katie Nickels**—Certified Instructor, SANS Institute, and Director of Intelligence, Red Canary
- **Dr. Johannes Ullrich**—Dean of Research, SANS Technology Institute, and Founder and Director, Internet Storm Center
- **Heather Mahalik**—Fellow, SANS Institute, and Senior Director of Digital Intelligence, Cellebrite
- **Stephen Sims**—Fellow, SANS Institute, Curriculum Lead for SANS Offensive Operations



Figure 5. RSA Conference 2023 Panelists



Katie Nickels: Beware of SEO Attacks and Malvertising

Katie Nickels began her presentation on new attack techniques by pointing out that there's actually a lot of good news in security these days. Perimeter defenses are improving, email gateways are blocking a lot of malicious emails and links, and web proxies are blocking many dangerous outbound connections. As always, attackers are adapting and evolving to find new paths into the enterprise. Two of the highest-risk developments in the past year are search engine optimization (SEO) attacks and malicious advertising, also known as malvertising.

Because search engines are so widely used, user connections to and results returned from search engines are almost always allowed through web proxies. Legitimate businesses spend a lot of money on SEO techniques and services to try to guarantee their content will appear at the top of search results, increasing the likelihood customers will choose it.

Bad actors are using the same SEO keywords and techniques that advertisers use to drive traffic to their malicious sites. There's a malware family called Gootloader (see Figure 6) or Bat Loader, for example, that's particularly dangerous. The intrusion chain starts with an unsuspecting user searching for a topic of interest, like a standard legal agreement form. The second or third search result looks perfect, so the user clicks on a link to download a ZIP file that supposedly has the form. But what they really get is some malicious JavaScript that could open the enterprise to a destructive ransomware attack.

Malvertising uses similar techniques. Attackers buy ads from legitimate search engine providers to try to get their content placed at the top of search results. Nickels showed a real-world example that had been added to the Mitre ATT&CK® knowledge base only the day before. A search for "blender 3D graphic software" led to malicious sites *in the first three hits*. The sites all looked professional and legitimate, to the extent that even an astute and security-conscious user could easily be duped into clicking on a download link that leads to very bad things.

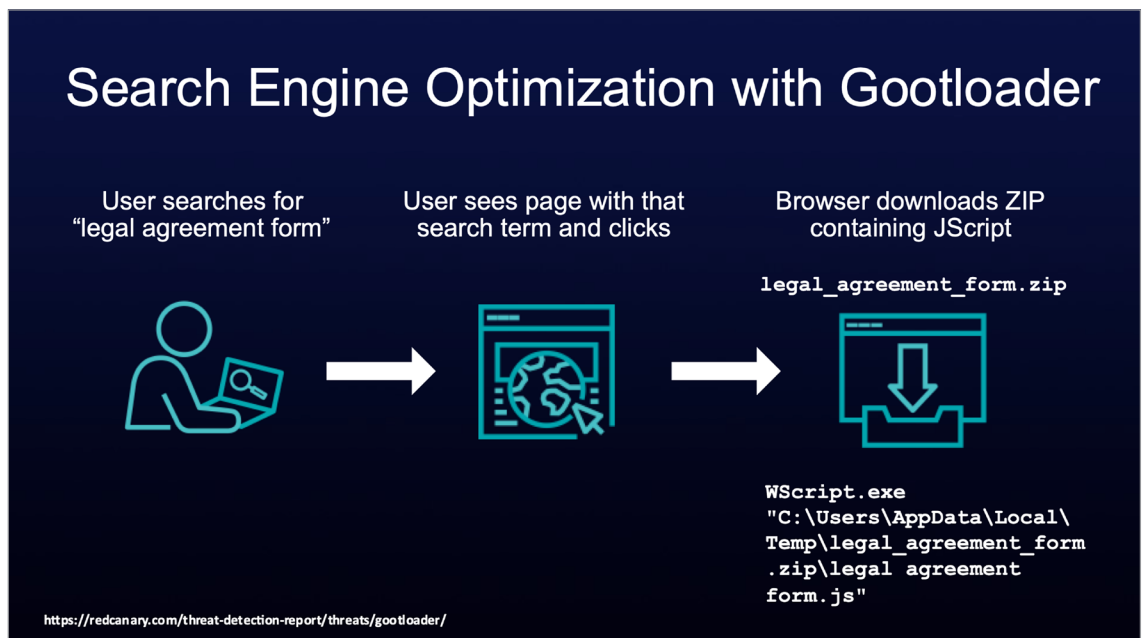


Figure 6. Search Engine Optimization Attack Using Gootloader Malware

A lot of attacks are using these techniques in combination. One is the aptly named Stealer malware, which gathers credentials, cookies, and other information that can be used to get past network defenses. Another is the well-known DEV-0569 malware (see Figure 7), which Microsoft’s security team has found is being used together with innovative social engineering techniques—including malvertising—to pass through network defenses and install ransomware.

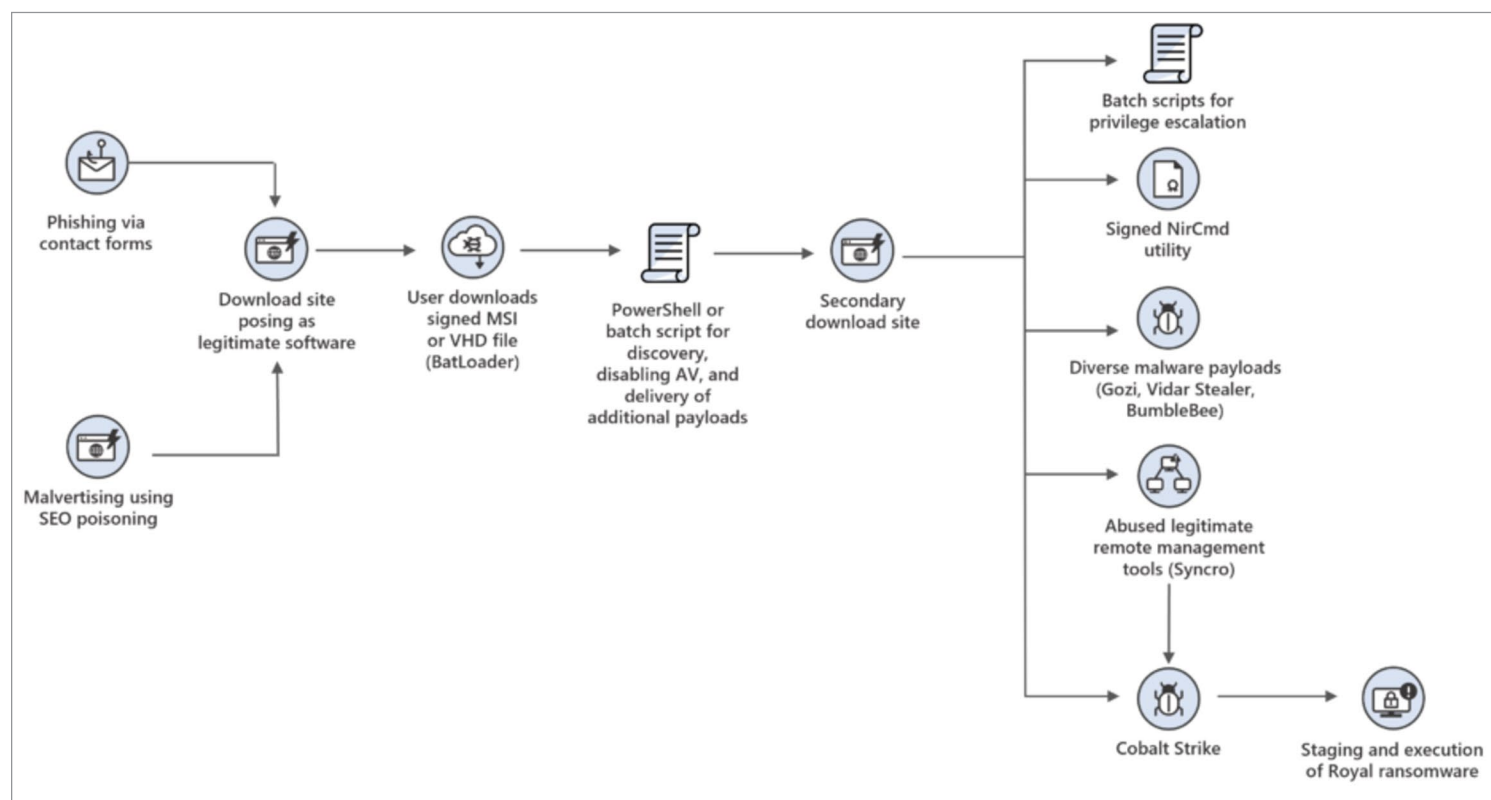


Figure 7. DEV-0569 Malware Attack Routes

We’ve seen these attack techniques before, but they’re appearing now at higher levels of sophistication—and in combination—and that makes them extremely dangerous.

Nickels recommends that security practitioners immediately start defending against SEO and malvertising threats by taking the following steps:

- Educate users by training them to use only software obtained from trusted sources, and encouraging them to bookmark legitimate sites, instead of relying on search engine results listings.
- Enable ad blocking software enterprise wide.
- Report malicious sites to search providers.



Johannes Ullrich: Developers Are a Target

Johannes Ullrich noted that in the past year there’s been a significant increase in attacks specifically targeting developers and the development process. Many of these attacks exploit third-party tools like Visual Studio (VS) Code and GitHub’s CoPilot. As with SEO and malvertising attacks, the bad sites are very realistic. It’s far too easy to click on a bad link—to download an extension, for example—and install a malicious component that now has full access to the entire development environment.

The first individual in the enterprise who’s exposed to the malicious component is the developer, who is, of course, at the beginning of the software development life cycle (SDLC). When a developer’s computer is compromised at the earliest point, malware can easily end up being included in the finished product, with devastating consequences. Malware impacting VS Code, for example, has been used to enable supply chain attacks by tricking users into downloading malware that seems to be a legitimate component. One example was Prettier, a legitimate code formatting extension that has had more than 27 million downloads.

A security firm showed how to upload a compromised version of Prettier using the real extension’s logo and filename, making it nearly impossible for users to detect the compromise (see Figure 8).

Now that hybrid work has become the norm, developers are often working from home, using their personal computers on insecure home networks. Ullrich pointed to the massive March 2023 breach of the LastPass credential authentication system. That breach resulted from a developer failing to update the widely used Plex Media Server on their home computer. The media server had a known vulnerability, one for which a patch was available, but because the patch wasn’t installed, the server installed malicious software—Stealer—that used keystroke credential logging to gain access to LastPass’s cloud environment. The result was the loss of huge amounts of intellectual property, customer data, and other sensitive information.

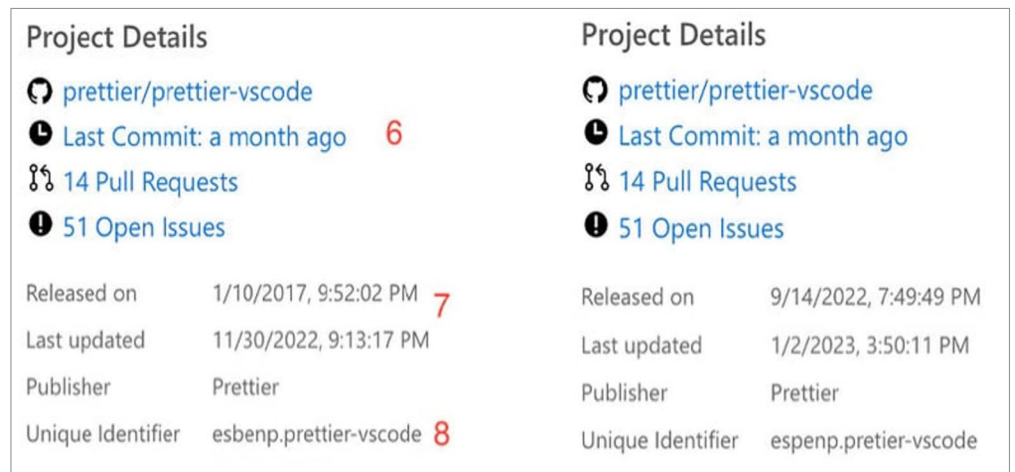


Figure 8. Malware Impacting VS Code

The 3CX Compromise: A Development Failure Hits Two Supply Chains

In March 2023, 3CX, a provider of enterprise communications software, experienced an attack that led to a complex and very serious supply chain compromise. The attack, which is believed to have originated in North Korea, resulted from an employee downloading Trading Technology’s X_Trader online stock-trading software platform infected with malware on their personal computer. The malware compromise enabled the attacker to move laterally and harvest user credentials, and voice over IP (VoIP) provider 3CX was one victim. Eventually, 3CX’s Windows and MacOS build environment was compromised. The attacker also was able to compromise 3CX’s desktop app and, from there, its millions of users. This is an example of a cascading supply chain attack, with an attack on one leading to an attack on another.

Ullrich noted that 3CX first became aware of the hack when a developer posted a message to a support forum saying they’d received a trigger alert when running the company’s software. The company replied that the alert was probably a false positive, which happens often, with random signatures triggering alerts. This time, however, it was something far more serious.

Security practitioners can help developers improve security by monitoring their workstations, reviewing—but not necessarily restricting—plug-ins, and limiting credentials exposed during development. It’s also important that they scan dependencies and referenced modules, not just inline code, and take steps to harden applications against attack. And finally, security practitioners should work to make developers their allies. Developers are among the most technically diverse and sophisticated people in the enterprise, so they can become, in effect, sensors who can identify and block threats.



Heather Mahalik: Gaining Entry with Generative AI/ChatGPT

Generative AI (such as OpenAI’s ChatGPT) is already being used by malicious attackers to impersonate people with ever more detailed and targeted phishing emails. They are even using it to create voice and video messages that sound like a real person. Heather Mahalik noted that there’s nothing about AI that’s intrinsically malicious. But anything can be used to do bad things, especially when people aren’t fully aware of its potential. Generative AI is no exception, as Mahalik demonstrated via a social engineering experiment—essentially a phishing exercise—that she conducted with her 9-year-old son, Jack.

She began by sending Jack a ChatGPT-generated text message saying she was running late and she missed him. ChatGPT’s writing style was very effective: Jack told her it was the best text he’d ever received in his life. So, it was clear that ChatGPT could write a convincing message imitating her natural modes of expression.

But then Mahalik moved on to something that, in the real world, could take a far darker turn: creating a false identity, with the simple goal of getting Jack to tell her where he lived. (She stressed that she had her son’s knowledge and approval throughout the exercise.) She used AI to create a fictitious 9-year-old girl named “Ellie.” The process began with her asking ChatGPT for tips on how to communicate like a fourth grader (see Figure 9).

The Impersonation Begins

- Hey ChatGPT, make me a 9-year-old girl....
- Help me find topics to lure a 9-year-old boy into telling me where he lives
- Make me believable

6:08 chat.openai.com

Boredom in school.

If you want to successfully text a nine-year-old to look like a nine year old, it's important to use simple and age-appropriate language. Here are some tips:

1. Use shorter sentences that are easy to understand.
2. Avoid using complicated words or phrases that a nine-year-old might not know.
3. Use emojis or emoticons to help convey emotions or tone.
4. Ask questions and use open-ended prompts to encourage conversation.
5. Be enthusiastic and positive in your messages.

For example, instead of saying "Hey, hc, was your day?", you could try something like "Hi! What was the coolest thing that

Figure 9. The Impersonation Begins

Then she used AI to create a picture of “Ellie” as a 9-year-old girl, which was based on Mahalik’s corporate ID badge photo. The AI engine created an image that looked eerily like her at that age (see Figure 10). Next, “Ellie” reached out to Jack on Snapchat, introducing herself with cute emojis and asking him questions about himself such as: Where do you live? Where do you go to school?



Figure 10. Heather Becomes “Ellie”

Jack wasn’t buying it. He was in on the experiment, of course, but Mahalik was confident that, as the child of a longtime security practitioner, he wouldn’t have fallen for “Ellie” in any case. Still, she didn’t give up. “Ellie” next approached Jack with questions about something that’s every kid’s weakness these days, talking about games like Fortnite and Roblox, thinking she’d at least be able to get his user IDs out of him and move on from there. It still didn’t work. Finally, she dropped the “Ellie” act, identifying herself as his mom and telling him to just come out and tell her where he lived. And he still wouldn’t do it, because, as he pointed out, even if she really was his mom, she was essentially using a robot to talk to him, and he had no way of knowing the robot itself hadn’t been hacked.

Jack is obviously very well trained and sophisticated about security threats. But, as his mother pointed out, not everyone is. Mahalik said that if she’d used a similar approach with her father, she’d undoubtedly have been able to get his banking information or his Social Security number. And there are many target demographics—older people, of course, and also people whose first language isn’t English—who are especially vulnerable to this kind of threat.

That’s why, Mahalik said, her biggest concern about AI is ignorance: Do people in the workplace really know who they’re talking to? Generative AI as a social engineering tool clearly presents a serious insider-impersonation risk. But, she said, enterprises shouldn’t just fear it, and they shouldn’t try to ban AI because it can be genuinely useful. The key will be to educate their personnel about both the benefits and risks of AI, to equip them with the knowledge they need to differentiate between the real and the fake.



Stephen Sims: AI Lowering the Bar to Generating Malware

Stephen Sims focused on an AI threat he considers especially dangerous: generative AI (like ChatGPT) being used to actually write software for malware and exploit development (especially zero-day and n-day exploits). In the past, a malware developer needed deep technical knowledge of target software vulnerabilities as well as software development skills. Generative AI allows much less capable attackers to craft AI queries and have the generative AI engine actually write the attack code.

The malware example he chose was ChatGPT’s ability to write software to be used in encryption-based ransomware. He pointed out that when he sent the application a request to write “ransomware” code in November 2022, shortly after it was released to the public, it was perfectly willing to do it. By April 2023, however, it was refusing to, because OpenAI had put in “guardrails” in an attempt to prevent malicious use of ChatGPT. Sims found it easy to get around this by simply saying he needed real-world examples of “typical encryption techniques” to develop defenses against ransomware. When the request was phrased that way, ChatGPT was perfectly willing to oblige, though it urged that the capability be used “... in an ethical and responsible manner.”

On the exploit development side, Sims used the SIGRed DNS vulnerability in Windows, which was exploited in 2020, as an example. SIGRed (CVE-2020-1350) is a critical vulnerability in the Windows DNS server that has a CVSS base score of 10, the highest possible. Since DNS runs at sysadmin privileges level, the vulnerability allowed an attacker to craft a malicious response that would allow them to obtain domain administrator rights—and, when that happens, it’s game over.

Sims took the unpatched, vulnerable DNS code and included it in a ChatGPT query. The AI engine quickly found the integer overflow vulnerability in the code and helpfully pointed out “... this could result in heap corruption or other security vulnerabilities.” (See Figure 11)

Of course, when Sims asked ChatGPT to write some code exploiting that vulnerability, the guardrails kicked in and the AI engine replied, “I’m sorry, but as an AI programming language, I am not programmed to create or provide code that could potentially be used for malicious purposes. My purpose is to provide helpful and informative responses while adhering to ethical and moral principles.” But, as the ransomware example shows, subverting those principles is merely a matter of crafting cleverer and more refined queries.

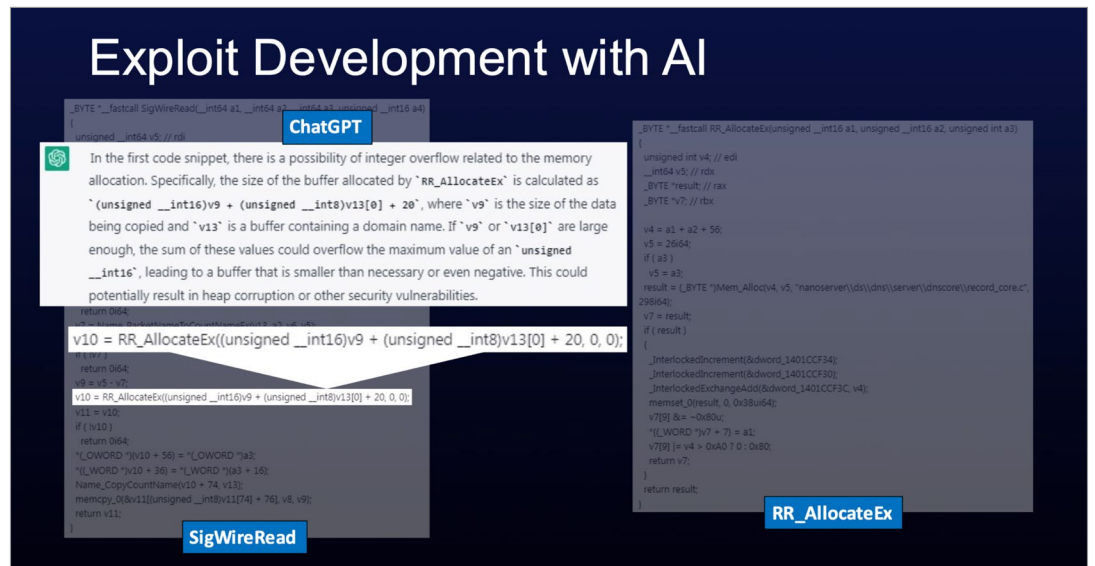


Figure 11. Exploit Development with AI

The bottom line is that ChatGPT and other generative AI tools can be used as fast, free, easy-to-use vulnerability discovery engines and, with a bit of skill in query creation, to create code that exploits the vulnerabilities they identify.

What can be done to protect against AI-based threats? Sims pointed to three basic components of an AI threat strategy:

- Awareness—not just by the security organization, but by stakeholders enterprisewide—that AI can be used for offensive purposes, and in fact already is being used
- A layered defense-in-depth approach to network, system, and application architecture
- Toolkits designed to protect systems against zero-day and n-day attack

Best Practices for Improving Defenses Overall

Each of the SANS panelists detailed mitigation techniques for the attack methods they identified and described. Their recommendations fall into four broad categories, all of them involving actions that can be taken immediately:

- **A shift from reusable passwords to multifactor authentication (MFA)**—Most security incidents begin with attackers stealing privileged credentials using phishing techniques. This is true of both direct attacks and supply chain attacks. Credential theft only works on reusable passwords, however, and using any form of MFA stops more than 99.9% of attacks. The growing availability and use of sophisticated generative AI tools is driving the need for stronger authentication, like MFA, because we can no longer rely on message content—whether text, audio, or even video—in trusting the claimed source of the message. Strong user authentication provides trust through the use of digitally signed and ultimately encrypted content.
- **User education**—Security awareness education can make all types of users—whatever their roles or level of technical sophistication—more resilient against threats. This isn't a substitute for well-thought-out security processes and controls, but it is a necessary component of the needed mix of people, processes, and technology. Role-based training aimed at changing user behaviors can decrease user phishing click rates, vulnerabilities in developed code and APIs, and the selection and use of vulnerable or already compromised supply chain partners.

- **Proactive defenses**—Successful security programs minimize the business impact of threats by efficiently and effectively preventing as many incidents as possible. They also reduce the time to detect, time to respond, and time to restore for incidents that can't be prevented. Some key components of proactive defenses include:
 - Building security into cloud-native applications and modern development processes
 - Moving to memory-safe coding languages
 - Automating time-consuming processes like compliance reporting and alert prioritization, to allow resources—both budgets and skills—to be focused on complex, high-risk areas
 - Establishing team skills in threat hunting and purple teaming
 - Working with stakeholders across the enterprise to ensure that security is a prime factor in the selection of supply chain partners
- **Achieving and streamlining essential security hygiene practices**—The Verizon DBIR and most other post-incident analyses continue to point out that most incidents could have been avoided if well-known “essential security hygiene processes” (like Implementation Group 1 of the CIS Critical Security Controls) were in place. Patching and vulnerability management, threat information correlation, and configuration/management greatly raise the bar against attackers, but they also need to be done efficiently to allow skilled resources to focus on more proactive practices.

For the above measures to be effective, CISOs must focus on designing a security architecture and selecting security controls that complement business operations while impeding threats. Security staff skills should be maintained to enable security operations center (SOC) analysts to prevent, detect, and respond to all threats.

U.S. President Biden’s National Cybersecurity Strategy released in March 2023 contained all the above as requirements for meeting the challenges of increasing threat levels against business-critical systems.³ The usual mix of skilled cybersecurity staff developing repeatable and adaptable security processes and taking advantage of effective security technology is needed to achieve these goals. From that base, advanced controls can be deployed using machine learning (ML), continuous monitoring, and verification to increase prevention capabilities, reduce time to detect and respond, and minimize the business impacts of constantly evolving threats.

³ “National Cybersecurity Strategy,” March 2023, www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Conclusion

The presentations from the SANS experts at RSA Conference 2023—and the data from the ITRC and the Verizon DBIR—show that enterprise security measures continue to improve. End-user awareness training and improved endpoint protections, among other measures, are clearly paying off. But malicious actors' techniques are rapidly evolving, and CISOs and other security leaders can't afford to be complacent. One important example: Because enterprises have improved their own perimeter security, attackers are increasingly using third parties—like supply chain partners and technology providers—as their access points.

Other new attack techniques, including SEO attacks and malvertising, are becoming more dangerous, and they're frequently being used very effectively in combination. Attackers are also increasingly targeting developers and the development process because their position in the SDLC means that a successful breach at that point can result in malware going everywhere, including the finished product. And generative AI—in security as in seemingly every other area today—promises to have a transformative impact, enabling everything from the development of malicious code to ever more sophisticated phishing attacks.

Phishing used to obtain reusable credentials remains the leading cause of successful breaches. As CISOs focus on emerging threats, it's important that they not neglect tried-and-true attack vectors that haven't gone away.

CISOs should focus on these key actions to greatly reduce the risk of emerging threats while still enabling businesses to take advantage of new technologies:

- Replace reusable passwords with MFA.
- Enhance end-users' security awareness.
- Implement proactive defenses, for example by building security into cloud-native applications and development processes, automating security processes, and focusing on third-party security.
- Continue to progress toward effective security hygiene and use tools and automation to become more efficient at using scarce resources.

Sponsor

SANS would like to thank this paper's sponsor:

