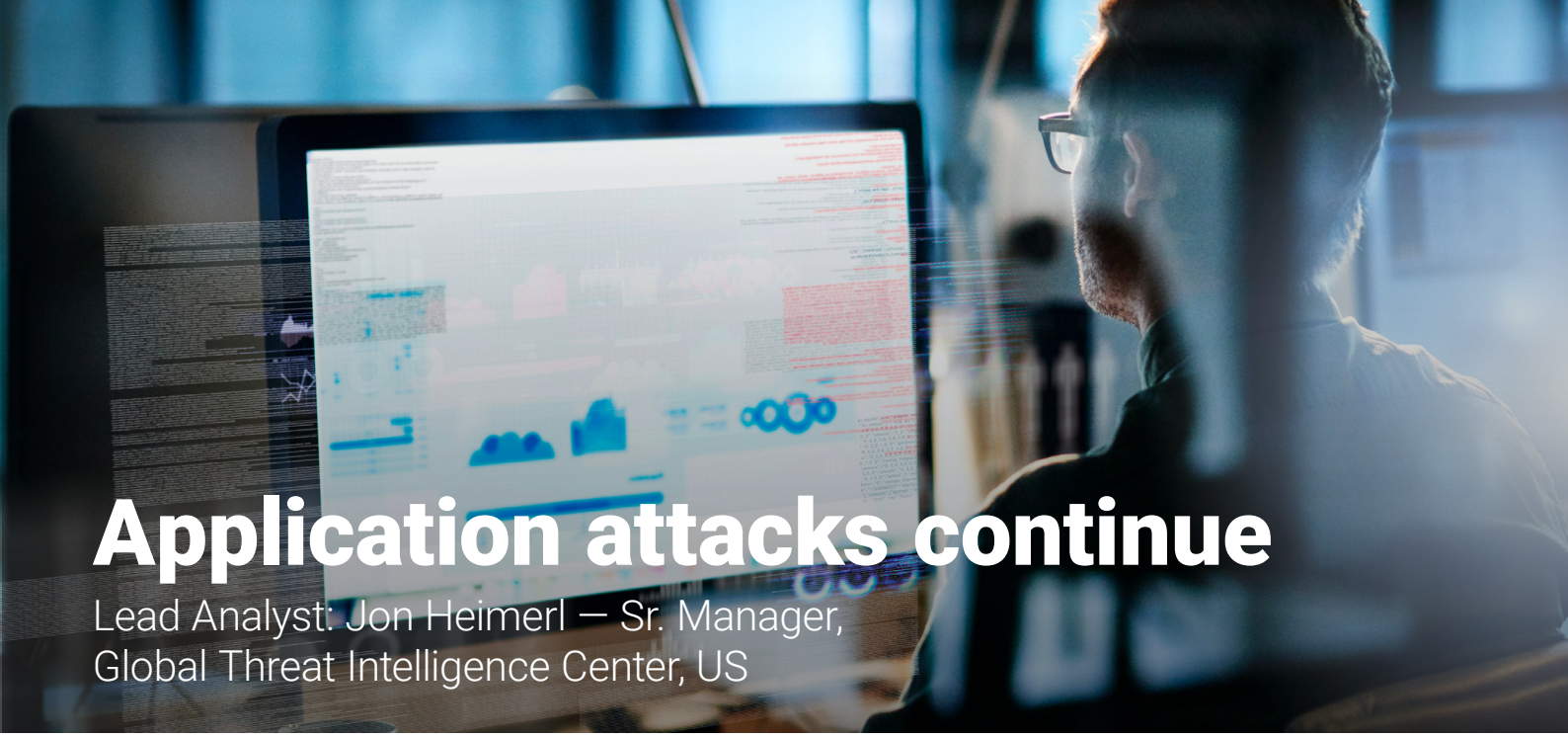
NTT Ltd. Global Threat Intelligence Center

Monthly Threat Report

August 2020

Contents



Application attacks continue

Lead Analyst: Jon Heimerl — Sr. Manager,
Global Threat Intelligence Center, US

Application attacks are a problem.

In 2019, about 55% of all attacks detected by our security monitoring services were either web-application or application-specific attacks. Through the previous few years, this hovered at around 30%.

What is an application attack?

Threat actors are attacking your applications; looking for flaws in the applications available through your web presence. But it's more complicated than that.

Application attacks occur in a number of ways. Threat actors are attacking off-the-shelf applications, custom-built applications, databases and support infrastructure, as well as development and management tools, along with additional implementations.

The actual application attack can be conducted with a variety of techniques, but ultimately, they have a relatively small set of goals:

1. **Gain access to the targeted system with a valid username and password.** The attacker would be able to log onto the target device with a username and password and perform any actions that user's privileges would enable. The biggest single advantage to this is that actions taken by what appears to be an authorized user are less likely to be flagged as suspicious in most organizations.
2. **Gain access to the targeted system through privilege escalation.** The attacker can exploit a vulnerability which allows them to act as if they have advanced privileges, even if they don't have the associated username or password. This attacker might execute code or change configuration settings which subsequently allow the attacker authorized access.
3. **Gain access to the operating system of the targeted system.** An attacker with 'admin' or root privileges can create users, install software (including malware like a remote access Trojan), and identify other systems susceptible to attack.
4. **Gain access to the database.** At the very least, this can result in the compromise of data in the database, as the attacker may be able to read everything. A user with active database access could potentially edit or delete data or tables, and potentially create new database users. This can easily lead to full data compromise and complete loss in the organization's confidence in the data.

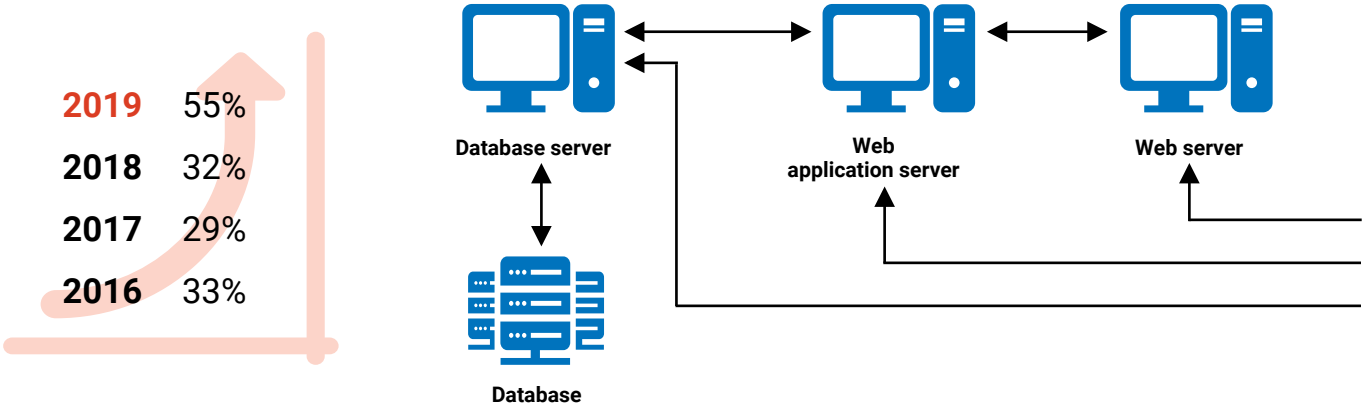


Figure 1: Percent of application attacks

Exactly what is being attacked?

According to data gathered for the 2020 Global Threat Intelligence Report, throughout 2019, 55% of all attacks targeted an organization's applications. The most attacked applications globally were primarily related to supporting the organization's web presence. Attacks targeting Joomla! (17%) and Apache products (16%) accounted for 33% of all attacks. Attacks against other content management systems and supporting technologies (e.g., noneCMS, IIS, Drupal, Oracle product, Adobe products, WordPress) accounted for another 19% of attacks.

In June 2020, attacks against networking products (i.e., Zyxel, Netis, Netcore, Netgear, Linksys, D-link and Cisco) and video cameras accounted for about 32% of all attacks. Many of these were brute force or authentication attacks.

But, beyond actual technologies being attacked, the list of actual vulnerabilities which are actively exploited tends to be relatively narrow. For instance, the top 10 most attacked vulnerabilities in 2019 accounted for 84% of all attacks observed and the top 20 most attacked vulnerabilities accounted for nearly 91% of all attacks.

This means that attackers tend to continue to use the exploits against vulnerabilities which are known to work. Exploits for most of these vulnerabilities are implemented into exploit kits or other tools which make it easier for the attacker to execute them.

The following table summarizes some of the vulnerabilities which are commonly attacked.

Application	Example CVEs	Summary description
Oracle Products	CVE-2019-2725	Some versions of Oracle WebLogic included a vulnerability which could allow an unauthenticated remote attacker to perform remote code execution on the targeted system. This could lead to exfiltration of data, modification of system files, loss of availability and more.
ThinkPHP	CVE-2019-9082	Some versions of ThinkPHP included a vulnerability which could allow an unauthenticated remote attacker to perform remote code execution on the targeted system. This could lead to escalation of privileges and allow the attacker to take control of the targeted system.
Joomla!	CVE-2019-9184	Some versions of the J2Store were vulnerable to SQL injection which could allow an unauthenticated remote attacker to run arbitrary SQL queries on the internal database. This could lead to escalation of privileges, the ability to extract or edit database contents and more.
	CVE-2015-8562	Some versions of Joomla! could allow an unauthenticated remote attacker to conduct PHP object injection attacks and execute arbitrary PHP code via the HTTP User-Agent. This could lead to exfiltration of data, modification of system files, loss of availability and more.
vBulletin	CVE-2019-16759	Some versions of the vBulletin platform were vulnerable to a remote attack which could allow an unauthenticated remote attacker to perform remote code execution on the targeted system. This could allow the attacker to install additional programs, view, change or delete data.
Apache Products	CVE-2019-0232	Some versions of Apache Tomcat running on Windows include a vulnerability which could allow an unauthenticated remote attacker to remotely execute arbitrary code. This could lead to escalation of privileges, install malware and potentially take control of the targeted system.
	CVE-2017-5638	Some versions of Apache Struts include a vulnerability which could allow an unauthenticated remote attacker to remotely execute code on the target system. This could lead of escalation of privileges, the ability to install malware and more.
OpenSSL	CVE-2014-0160	Some versions of OpenSSL are vulnerable to the Heartbleed vulnerability, which allows unauthenticated remote attackers to obtain sensitive information from process memory via specially crafted packets which force a buffer over-read. This can lead to the disclosure of private or sensitive information.
IIS	CVE-2017-7269	Some versions of IIS are vulnerable to an error in the way WebDAV handles objects in memory, exposing the system to a vulnerability which could allow an attacker to run arbitrary code on the targeted system. This can lead to the attacker gaining the same user rights as the current user, resulting in complete loss of system control including compromise of all data.
WordPress	CVE-2020-7048	Some WordPress installations use the WP Database Reset plugin which has a vulnerability allowing an unauthenticated remote user to use the plugin to reset any database tables. This can lead to a full website reset or takeover.
	CVE-2019-6703	Some WordPress installations use the Total Donations plugin which has a vulnerability allowing an unauthenticated remote attacker to arbitrary update option values. This can lead to disclosure and editing or deletion of data as well as site takeover.

Table 1: Technologies targeted for some 40% of all application attacks we observed

So, what do I do about it?

Since organizations continue to develop new web-enabled apps to support their business, this is not a threat which will be easily eliminated. However, there are some actions an organization can take to help manage their exposure due to application attacks.

1. Ensure you maintain an effective secure development program. Include a training program to help developers learn and use secure design and coding techniques, and support that program with mentoring, tools and continued training. Many developers are not trained in security, and there are techniques which can potentially reduce vulnerabilities which are built into custom applications, making those applications more resilient and less error prone.
2. Patch or update your environment, at least in the critical or internet-accessible systems. If you are using any of the applications listed in the table, you should make sure they are on the latest patch level. While it's not exciting, proper patching may be the single most effective protection against application attacks. Keep in mind that the technologies listed in the table account for about 41% of all attacks we observed in June 2020. So, if you can patch these, you have made significant progress eliminating targets of which attackers may try to take advantage.
3. Add a web-application firewall (WAF) to help protect your exposed systems from attacks. A decent WAF can help block or filter attempted attacks, and alert you that you are being attacked. A WAF can block activity from potentially hostile sources and can identify exploit attempts.
4. Segregate your internal environment. Attackers commonly compromise a single host, then spread from that host to other systems in the organizational environment. Even when they don't continue lateral compromise through the environment, that original system becomes a source of attacks of other systems and potential hostile accesses. Segregation of internal networks from each other using access control lists, white lists, blacklists and other filtering techniques can help limit, or at least interfere with, the attacker's attempts to access other systems and data from any compromised system.
5. Use the least privileged account you can and still allow viable use of an application. Many exploits grant the attacker the privileges of the attacked user, or the privileges with which the application is running. If the application is running under an 'admin' family of privileges, which can grant the attacker a greater level of control in the organization's environment. You want applications to run with the permissions of the lowest possible user, or better yet, define a specific account for the exact privileges the application will require. Then monitor for non-standard activity from what should be a very predictable account.
6. Test your applications. Despite all the other actions you have taken, if you test your application environment, especially your web-enabled applications, you get the chance to potentially identify and fix any problems before an attacker gets the chance to identify and exploit them.

Application security encompasses a vast set of controls and concerns and starts with designing secure applications, considering security as a basic business requirement, and extending good security practices through ongoing testing, maintenance and monitoring of the supporting operational environment. Application security is a complex problem. But understanding potential impacts on your organizational environment and prioritizing what is important to the organization is an excellent first step in managing risk.

Keep in mind that **just eight technologies** (see Table 1) account for about **41% of all attacks** we observed in June 2020. If you can patch these, attackers have far fewer targets they can take advantage of, **significantly lowering the risk of attack.**

Consolidating cyber

Infosec incentives for vendor partnerships

Lead Analyst: Haydn Bowers — Security Architect, Solutions, Australia

There are three key pillars within information security: people, process and technology. While as technologists, we're conditioned to design and deliver 'best-of-breed', we've noticed a significant market trend. Organizations are no longer looking for the greatest technology but are considering a unified strategic approach partnering with vendors who provide effective coverage of security controls.

According to an article on helpnetsecurity.com, organizations average 80 different security vendors within their organization.[1] Our Security Controls Dashboard, part of our Cyber Advisory consulting assessments, counts 67 information security controls. People, processes and technology must be considered across each to maintain an acceptable level of cyber maturity. There is, of course, a risk in trying to be 'too secure' or emphasizing controls which might be beyond what is truly appropriate for the organization. If an organization was to consider a 'best-of-breed' technical control for each, they introduce unnecessary risks in maintaining expertise, providing an integrated architecture and potential for an undefinable budget.

Reviewing the results of Cyber Advisory engagements and the efficiency of security programs analysed, helps identify three areas in which improved management of vendor relationships can make those security programs more effective:

- **People are the greatest variable** within any organization's risk management framework. But it's important to remember that 'people' does not just mean 'security awareness'. Multiple technological controls require staff to achieve and maintain a greater set of skills to implement, operate and analyse supported technology. Obtaining technical capabilities for project and operational teams significantly increases personnel risks requiring siloed expertise and increasing training costs, leading to ever-diminishing returns. Managing the required in-house expertise for a plethora of vendors increases the complexity of security personnel management. The potential to reduce personnel management with consolidated vendor partnerships enables security managers to reduce risk in their operations.
- **Process automation and orchestration** is an essential component to a cyber-security strategy. This is true from orchestrated detection and response, delivered from Security Orchestration, Automation and Response (SOAR) technologies, to enabling rapid time-to-value using deployment automation within consolidated technological investments. Security controls should be coherent and consistent, enabled by the integration of appropriate technology to the extent practical. The consolidation of multiple vendor technologies by addressing a greater set of cybersecurity controls in a single suite or unified solution can streamline the ability to integrate technologies to automate and orchestrate previously manual processes, while simplifying security management.

Information security must be considered holistically, taking business strategy and risk management into account within an enterprise security architecture.

[1] https://www.helpnetsecurity.com/2018/03/30/too-many-cybersecurity-companies/

- **Technological consolidation within information security** dismisses a previously held technocratic notion that 'best-of-breed' technology is required to best defend an organization's critical assets. Organizations often realize a diminishing return-on-investment made with each additional purchase of security technology. This makes it increasingly harder for CISOs to justify additional budgetary spending. Information security must be considered holistically, taking into account business strategy and risk management within an enterprise security architecture. From this position, an organization's security architect can align with a vendor which meets the prioritized controls within the security strategy. This alignment can help increase the organization's purchasing power; reducing the overall security spend whilst still achieving the required security outcomes. This approach may not necessarily provide 'best-of-breed' technical controls but improved integration, unified management solutions and partnerships can increase the effectiveness of controls within the organization, and consequently, the overall security maturity. This enables organizations to increase their security maturity with less complexity and cost.

Effective vendor partnerships and the implementation of a smaller set of tools which support a 'secure operating platform' can improve an organization's ability to manage risk. This approach simplifies risk management practices, reduces the complexity of tool management and can help increase the cyber maturity of an organization. The three reasons to consider a consolidation of vendors for cybersecurity solutions are:

1. Reduction in risk for both the vendor and the operating environment
2. Greater coordination of processes
3. Increased purchasing power

With reduced IT spend being predicted as an outcome of COVID-19, the adage **'architect twice, implement once'** is going to be even more imperative.

#Spotlight 2

Secure by design:
An application perspective

Many organizations rely on custom applications for key aspects of their business. Unfortunately, designing, building and maintaining a secure application is not an easy task.

Attackers are aware of this: our 2020 Global Threat Intelligence Report identified that nearly 55% of attacks we detected were application-specific or web-application attacks. Secure design is critical for public-facing applications, but even internal applications can be exposed to insider threats or external attackers who are able to gain access through other means (e.g., compromised credentials or infecting workstations with malware).

Many applications can be exploited using a few well-known techniques, no matter how unique the functionality of your specific application is. This is because developers tend to make the same types of mistakes; the easiest or most obvious way to write an application function is often not inherently secure. Teaching developers to understand and avoid creating these types of vulnerabilities is one critical step towards creating a secure application. The OWASP Top Ten catalogues these common critical vulnerabilities and should be a key resource for developers.

Secure by design goes beyond day-to-day coding, however. Important decisions must be made during the design phase that will determine the overall risk that the application poses and how it's mitigated. The following topics should be considered during the design phase:

- Development managers should consider creating code libraries for critical functions within the application that could otherwise introduce vulnerabilities (e.g. user input, authentication, database access, file access) so they can be thoroughly reviewed and vetted. Developers should be required to use these libraries not only for consistent coding practices, but to avoid introducing errors.
- Applications should not collect or store unnecessary sensitive data. Data which hasn't been collected can't be compromised by an attacker. Any sensitive data gathered temporarily should be expunged when it's no longer needed to reduce the amount of data an attacker can quickly collect during a breach.
- If sensitive data is collected it should be encrypted. This includes encrypting data at rest when it's stored in a file or database and when it's in transit between the application and the user or other connected systems.
- Don't let developers 'reinvent the wheel' for security critical processes like encryption and authentication (including 'lost password' functionality). Your development team should be using encryption and authentication processes that have been publicly vetted for security. Any attempt to 'build it yourself' is almost certain to result in the same mistakes others have already made (and learned from).
- An attacker may be able to find a way to compromise your application even if you've implemented good security precautions. Applications should be designed to generate alerts when they encounter unexpected inputs or conditions and these alerts must be investigated seriously and promptly.
- Developers will always make mistakes; they're human after all. Conducting regular penetration testing of an application will help find vulnerabilities which slipped through internal testing, before they are found by an attacker. Remember to prepare for long term maintenance of your application as well, since you never know when a new vulnerability will be discovered that requires a fix.

And remember, as in all things related to information security, there is no single bullet – no 'one-size-fits-all' solution. Organizations should consider the effectiveness of their existing controls and evolve towards a more secure environment. Considering the controls listed here can help manage that process in an efficient manner and can help integrate secure by design principles into your software development processes.

NTT Ltd.'s Global Threat Intelligence Center

The NTT Ltd. Global Threat Intelligence Center (GTIC) protects, informs and educates NTT Group clients through the following activities:

- threat research
- vulnerability research
- intelligence fusion and analytics
- communication to NTT Group clients

The GTIC goes above and beyond the traditional pure research organization, by taking their threat and vulnerability research and combining it with their detective technologies development to produce applied threat intelligence. The GTIC's mission is to protect clients by providing advanced threat research and security intelligence to enable NTT Ltd. to prevent, detect and respond to cyberthreats.

Leveraging intelligence capabilities and resources from around the world, NTT Ltd.'s threat research is focused on gaining understanding and insight into the various threat actors, exploit tools and malware – and the techniques, tactics and procedures (TTP) used by attackers.

Vulnerability research pre-emptively uncovers zero-day vulnerabilities that are likely to become the newest attack vector, while maintaining a deep understanding of published vulnerabilities.

With this knowledge, NTT Ltd.'s security monitoring services can more accurately identify malicious activity that is 'on-target' to NTT Group clients' infrastructure.

Intelligence fusion and analytics is where it all comes together. The GTIC continually monitors the global threat landscape for new and emerging threats using our global internet infrastructure, clouds and data centers along with third-party intelligence feeds; and works to understand, analyse, curate and enrich those threats using advanced analysis techniques and proprietary tools; and publishes and curates them using the Global Threat Intelligence Platform (GTIP) for the benefit of NTT Group clients.

Our **Global Threat Intelligence Center** goes beyond a traditional research-only approach by combining focused research with detective technologies. This results in **true applied threat intelligence** to protect our clients with effective tools and services which reduce security risks and threats.

Recent assets

2020 Global Threat Intelligence Report

The 2020 NTT Ltd. Global Threat Intelligence Report (GTIR) is the culmination of the data the Global Threat Intelligence Center gathered and analyzed throughout the year. We produce this report by collecting a broad set of global data (log, event, attack, incident and vulnerability) to identify key cybersecurity trends of which businesses need to be aware.

Download report

If you haven't already, **register to receive the Monthly Threat Reports** directly to your inbox each month.


NTT