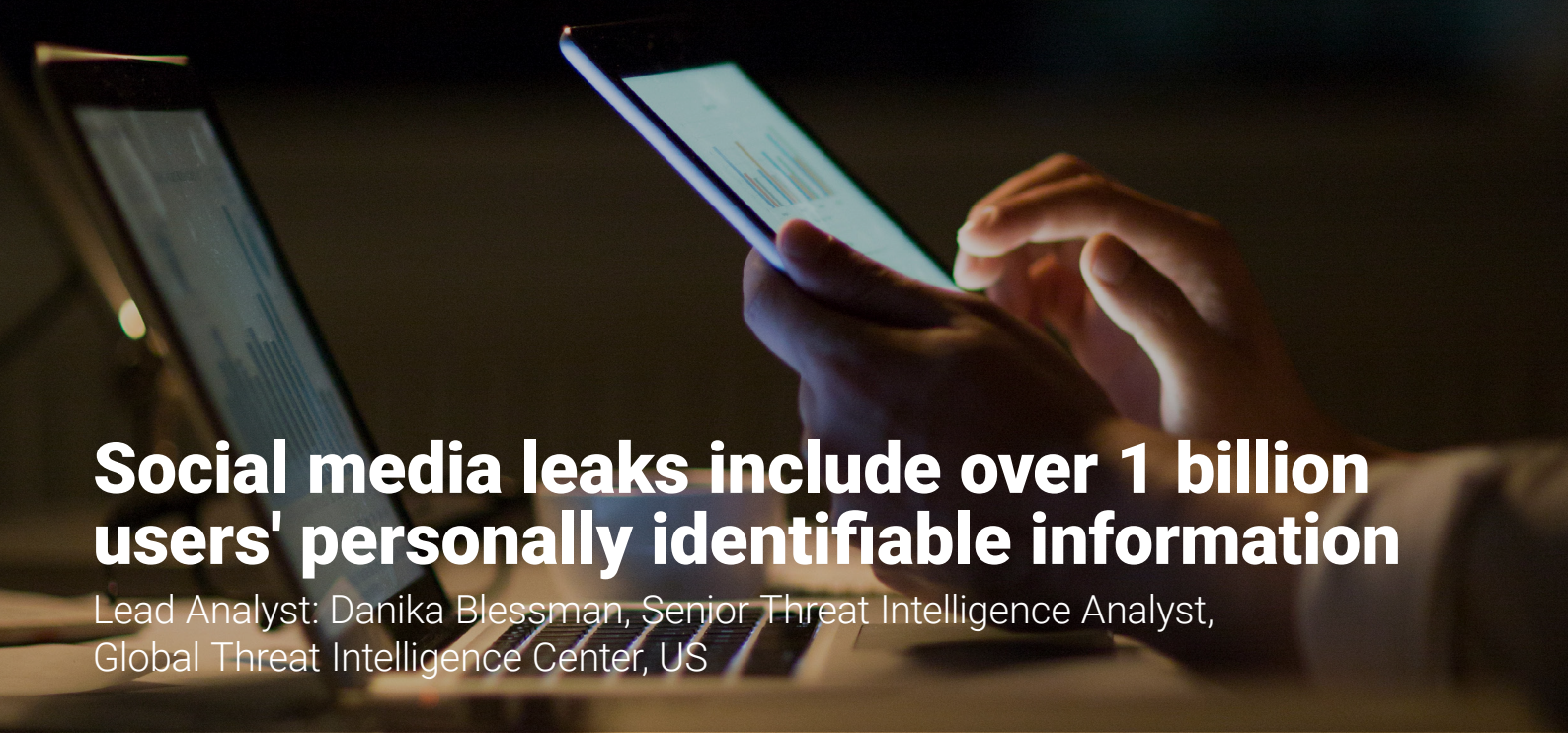
Global Threat Intelligence Center

Monthly Threat Report

May 2021

Contents



Social media leaks include over 1 billion users' personally identifiable information

Lead Analyst: Danika Blessman, Senior Threat Intelligence Analyst, Global Threat Intelligence Center, US

Social media can be a great source of information, disinformation and often oversharing of information. It's also a great source of personally identifiable information (PII), lucrative not just to marketers, but to threat actors and cybercriminals.

Over the past few weeks, two prominent social media firms – or, rather, their users – became the victims of a data leak/scraping attack using publicly known techniques.

Initial reporting from Business Insider revealed that over 533 million Facebook users' PII - including phone numbers, birthdates, email addresses and locations – were leaked online. This leak appears to have affected users across over 100 countries; those with the highest number of impacted users are the US (32 million), the UK (11 million) and India (6 million).

Facebook reported the data was scraped using a vulnerability available as early as 2016, which Facebook says was patched in 2019. While the data leaked appears to be several years old, the age of the data does not preclude it from being effectively exploited by various threat actors. Most users have not changed their contact information since the leak, leaving them open to potential phishing and scam campaigns.

Hot on the heels of the Facebook leak, LinkedIn announced that over 500 million of its 740 million users were the victims of a similar scraping of PII.

The more significant issue, though, is that when an organization's primary asset is data, that data could be valuable to more than just you or your organization – or to the initial threat actor or cybercriminal. Stolen data can be passed from one criminal group to another, or one cybercriminal group might not protect their data, allowing it to be further compromised. And, if threat actors are targeting a specific organization – perhaps, via a supply chain or third-party attack – simply knowing email addresses or phone numbers can easily be an avenue for social engineering attacks.

The greatest risk to these users is likely an uptick in fraud and other social engineering campaigns – including phishing attacks – from various threat actors and cybercriminals.

Additionally, the leak of this type of PII could lead to an increase in robocalls or spam text messages, both of which are already huge issues, leading to the potential for affected users or organizations to reveal further information via these robocalls or spam texts. Attackers are using tools to support phishing or business email compromise attacks. If attackers can find, trade or buy information about their victims, it can make automated attacks even more effective. Additionally, attackers have used such information to support brute-force and credential-stuffing attacks as attackers try to take advantage of what they already know about the users.

From a security standpoint, individuals and organizations alike need to be aware that their data is already out in the open. Still, they need to remain vigilant about the potential for phishing or fraud using their leaked data. The recent social media leaks are not the only ones individuals or organizations will encounter, nor will they be the last. The truth is that data breaches have, unfortunately, become fairly common for a wide range of online services. Unless you rarely use the internet or mobile apps, it's likely your personal information is already in the hands of cybercriminals.

The bit of good news is that the PII exposed in this leak are not the most useful to attackers or cybercriminals, unlike data such as credit card information or social security numbers.

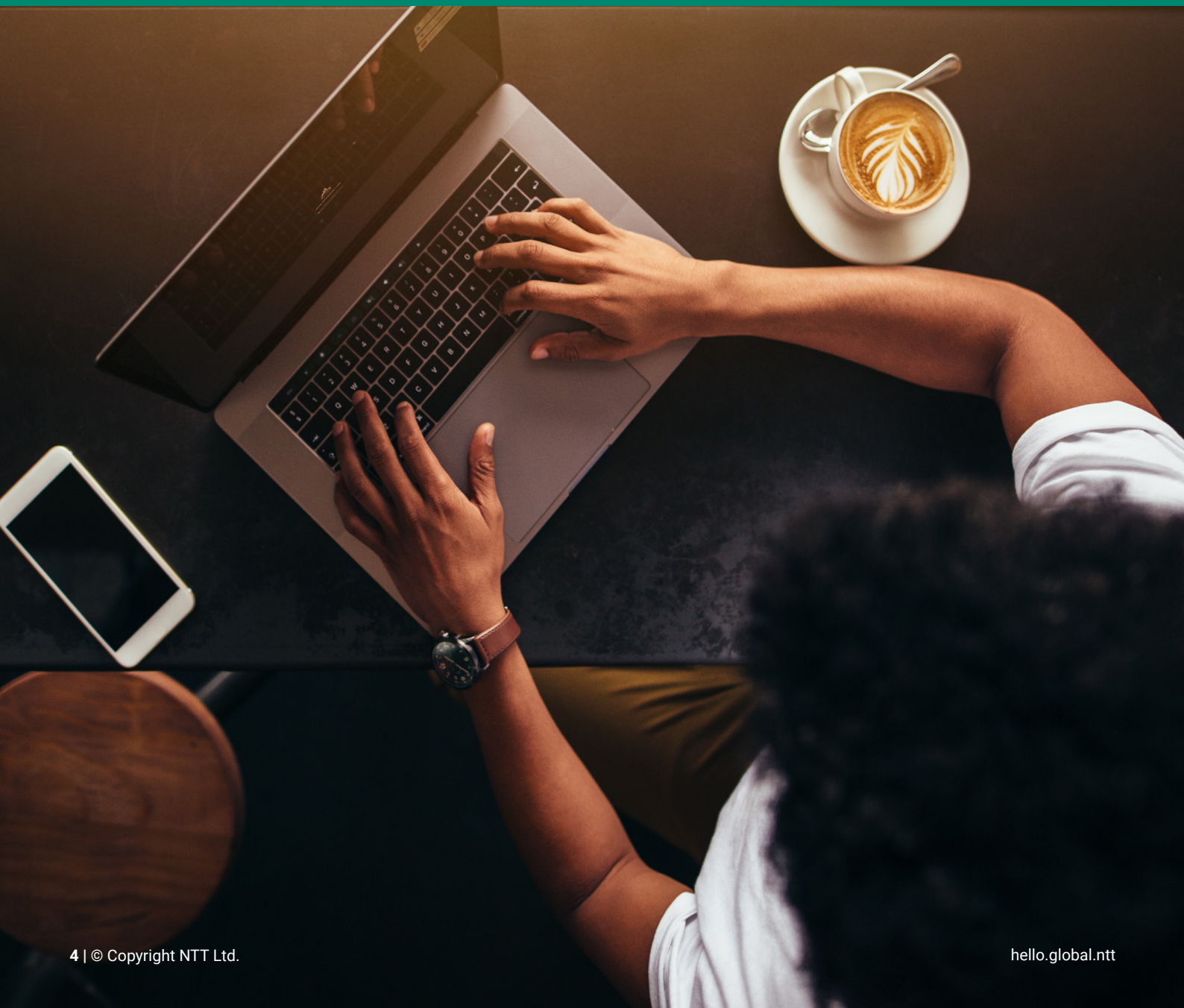
Aside from using the phone numbers and email addresses gleaned for future phishing/spamming campaigns, those affected should continue best security practices and maintain awareness regarding accounts.

If you discover your information has been leaked or compromised, all is not lost, there are several things to reduce the threat from these types of data breaches:

- Continue to implement best security practices and common sense.
- Enable two-factor authentication (2FA) on websites that allow this security feature.
- Change your password on Facebook and other websites on which you may have reused your password or login credentials.
  - Change these frequently for each website and use different passwords for each account you have.
- Be aware that your phone number and email address are likely in the hands of cybercriminals or threat actors.
- Do not give out PII to anyone who calls you claiming to be from a financial institution, doctor's office, etc., instead, call back to a trusted number to verify they have contacted you.

Mostly, though, users need to be aware of what information they are putting on the internet – in this case, social media platforms. Multiple seemingly insignificant pieces of information could, in addition to being financially lucrative to cybercriminals, potentially put a user in harm's way by giving away workplace, home information, photo or information on their children, family and friends.

Unless you rarely use the internet or mobile apps, **it's likely your personal information is already in the hands of cybercriminals.**



ThinkPHP is a hot target

Lead Analyst: Jon Heimerl, CISSP, Senior Manager,
Global Threat Intelligence Center, US

According to data gathered for the GTIC 2021 Global Threat Intelligence Report, ThinkPHP was the single most targeted technology in 2020, targeted in 30% of all attacks directed at an identifiable technology. In 2019, ThinkPHP was not even in the top 20 most targeted technologies and accounted for less than half a percent of global attacks.

ThinkPHP is a free web development framework. It is based on PHP and distributed under an Apache2 open-source license. It was designed to support the development of enterprise projects while prioritizing simple code that resulted in a strong performance. Organizations who embraced ThinkPHP realize efficiencies in the development process for web-enabled applications.

ThinkPHP supports many content management suites (CMS), private and public websites, and public applications such as ECShop. As a web development framework, ThinkPHP operates in the same market as Microsoft ASP.NET and Ruby on Rails, but on a smaller scale. ThinkPHP has a market share of less than 0.2% globally, but it is popular in some development communities, especially in China. Website statistics have been varying greatly for ThinkPHP.

Vulnerabilities in ThinkPHP have been problematic for some time. In 2018, researchers identified five different vulnerabilities in ThinkPHP, all involving SQL injection, and all with a CVSS of 7.5. Exploitation of these vulnerabilities did not require authentication and could have led to loss of system integrity.

Targeting of ThinkPHP gained popularity among hostile threat actors with the release of exploits of an additional vulnerability.

Vulnerability exploitation is not complex and requires little skill to execute.

CVE-2018-20062

CVE-2018-20062 is a remote code execution vulnerability originally discovered in a ThinkPHP library used in NoneCMS v1.3. ThinkPHP versions up to and including v5.0.23 are vulnerable.

Since user input was not being properly sanitized, the vulnerability allows an unauthenticated user to execute arbitrary PHP code. Worse yet, exploitation is not complex and requires little skill to execute. Successful exploitation could lead to remote takeover of a vulnerable server, making the CVSS of this vulnerability 9.8. Active exploitation began only days after researchers published proof of concept code.

Attackers quickly weaponized exploits and began scanning for the vulnerability. Attackers also implemented scanning and exploitation attempts into botnets, especially Mirai and derivatives, which attempted to use this exploit for propagation and DDoS attacks. They scanned for vulnerable servers and executed dictionary attacks against identified web servers to facilitate additional compromise.

It may be interesting to note that during 2020, while Mirai detections in the Americas and EMEA accounted for less than 1% of all malware, in APAC, Mirai accounted for over 8% of all malware. Over the past few months, analytics have not shown vast numbers of websites using ThinkPHP, but typically about 65-75% of those sites are located in APAC, most of them in China.

The good news is that CVE-2018-20062 was patched in December 2018. Organizations who have not applied the patch are likely still vulnerable. Given that the patch was available in 2018 and ThinkPHP was still the most attacked technology in 2020, it is worth organizations taking another look at whether they are still vulnerable.

For more information about the impact of ThinkPHP and the threat landscape, read the 2021 Global Threat Intelligence Report, which will be published on 11 May 2021.

NetSupport Manager is a **RAT!**

Lead Analyst: Jeannette Dickens-Hale, Senior All-Source Threat Intelligence Analyst, Global Threat Intelligence Center, US

The 2021 GTIR research data show that NetSupport Manager was the most commonly detected remote access trojan (RAT), at 6% of global activity.

A remote access trojan (RAT) is malicious software that allows a threat actor to gain unauthorized access to a victim's computer. RATs are known for their longevity. They can remain hidden to avoid detection, then spread other malicious malware laterally across the infected system. Remote access trojans have become powerful tools in cybercriminals' and nation-state hackers' tool kits.

GTIR data show that at 13%, NetSupport Manager was also the second most detected malware in the Americas. At the same time, this RAT did not appear in the top five malware categories in other countries that the report referenced. It's essential to note that the healthcare industry had nearly 57% of all malware activity via NetSupport Manager.

NetSupport Manager is legitimate software that has been used via phishing campaigns with COVID-related themes or fake notifications to entice victims to open a malicious attachment, to click on an online advertisement, or through social engineering – pretending to send information from a trusted source. It's important to remember that NetSupport Manager is a legitimate administrative RAT which is why it is widely distributed among cybercriminals and has become a favored vehicle to launch attacks against unsuspecting victims.

RATs, such as NetSupport Manager, are stealthy and can be difficult to detect once installed as they do not usually appear in a list of programs running on a computer. We recommend following best practices to strengthen an organization's security systems. System owners and administrators should review any configuration changes before updating security protocols. Best practices to mitigate malware breaches include, but are not limited to the following steps:

- Maintaining up-to-date antivirus signatures and engines.
- Ensuring systems have the latest security updates.
- Disabling file and printer sharing services. (If these services are required, use strong passwords or Active Directory authentication.)
- Restricting users' permissions to install and run unwanted software applications.
- Enforcing a strong password policy.
- Exercising caution when opening email attachments.
- Enabling a personal firewall on agency workstations that is configured to deny unsolicited connection requests.
- Disabling unnecessary services on agency workstations and servers.
- Scanning for and removing suspicious email attachments.
- Monitoring users' web browsing habits.
- Exercising caution when using removable media.
- Scanning all software downloaded from the internet prior to executing.
- Maintaining situational awareness of the latest threats and implementing mitigating controls.

After scrubbing infected systems, change all passwords and check all computers connected to the infected network to ensure no infections exist.

For more information on NetSupport Manager, RATs and the threat landscape, read the 2021 Global Threat Intelligence Report, which will be published on 11 May 2021.

Remote access trojans **have become powerful tools** in cybercriminals' and nation-state hackers' tool kits.

NTT's Global Threat Intelligence Center

The NTT 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 to prevent, detect and respond to cyberthreats.

Leveraging intelligence capabilities and resources from around the world, NTT'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'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

Our 2020 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