NTT Security

GTIC Monthly Threat Report

November 2018

Holiday Edition

Contents

NTT Security

Protecting Yourself During the Holidays

Lead Analyst: Jon Heimerl

Cybercrime is a multi-trillion-dollar industry. Financial fraud costs businesses and consumers trillions of dollars annually. Vulnerabilities are up – attacks are up. Cybercriminals show no sign of slowing down or giving up. Crime is profitable.

According to the NTT Security 2018 Global Threat Intelligence Report, the retail industry was the fifth most targeted industry globally – being the target of about eight-and-a-half percent of all attacks. But that percentage is a little misleading, since that number may not include attacks in which consumers are attacked directly. Much of the activity which relates consumers to the retail industry is credit card fraud.

In general, the retail industry expects fraud attempts to increase during the holiday season, and 2018 is no exception. Fraudulent transactions mirror sales numbers – as sales goes up, so will fraudulent activity. Consumers are also directly targeted by fraudulent activity as cybercriminals attempt to capture their card details or entice them to be victims of the various scams, with which we have become all too familiar. Businesses have a variety of controls for which they are responsible – hardening systems, applying patches, training employees, and implementing layers of related controls to help mitigate attacks against their organization. At the same time, there are positive actions which consumers can take to reduce the likelihood they will be impacted by cybersecurity threats and fraud during the holiday season.

The first step is understanding that consumers *are* being targeted.

1. Cybercriminals use your card details for their own purchases, like buying services or products, or buying high-demand products and selling the product on the secondary market to launder the money.
2. Cybercriminals can sell validated credit card numbers for $30 or more. So just having your card number can be valuable – especially if you consider that cybercriminals aren't just selling *your* card; they are selling yours and 30,000 others, or even yours and 300,000 others. Selling credit card information is a very lucrative business.

The second step is reducing the chances you will be targeted, and if you are targeted, mitigating the impact.

1. **Shop from your own device, not a borrowed or public device like at the business center at a hotel.** You can't rely on the security someone else has put in place.
2. **Don't shop over public Wi-Fi unless you are using a secured VPN (virtual private network) which secures that connection.** Using that unprotected Wi-Fi increases the chances that cybercriminals can monitor your communications and intercept account passwords or credit card numbers.
3. **Shop at reputable sites.** Stick with brand name sites you recognize.
4. **Don't click on links in emails.** The use of phishing emails is one of the most common attacks used by cybercriminals. Studies indicate that victims tend to open phishing emails between 25 and 30 percent of the time, so attackers continue to use them. You may receive a legitimate looking email, from what appears to be a legitimate retailer, but deciding to click that link

dramatically raises the risk that you will be successfully targeted by such an attack and exposed to a variety of malware and other attacks. It may be slightly less convenient, but you are almost always better off manually typing in the store's URL.

5. **Only enter your credit card details into secure sites.** If the site does not support HTTPS (or does not show the lock on the browser window) it is possible for cybercriminals to intercept the credit card information you enter. That indicates the site has made a conscious decision to NOT support good business practices and additionally may very well be a fraudulent site.
6. **Use a credit card instead of a debit card.** Most credit cards have lower fraud limits, which helps limit the amount of money (if any) for which you might be responsible.
7. **Many credit cards allow you to set limits and thresholds from your online account.** For instance, you might set a limit on a single transaction of $500, or you can request verification of such a transaction. So, a $500 charge is either automatically rejected, or it generates a text message, or message to the card's mobile app, which allows you to manually authorize the transaction. This can improve the chances you will recognize attempted fraud exactly when it happens and can limit the size of the impact.
8. **Make sure your own system is secure.** This applies to whatever system you are using to shop. While not everyone can harden a system, there are basic controls which are available to pretty much any user. Apply patches and upgrades and ensure whatever malware solution you are using is up to date. These actions can dramatically reduce the number of ways a cybercriminal has to attack your device.
9. **Use good online practices.** This one is harder, but the important part can be condensed into a single statement: use good passwords. Every important online site which holds your credit card or other important data should have their own, unique password. While it is impractical to make those passwords random, it is not difficult to make them practical. The danger in overusing the same (or similar) passwords is that if a cybercriminal captures your password for a particular retailer, then all sites at which you use that same password are now vulnerable to that same cybercriminal accessing your data.
10. **Check your credit card statements regularly.** During the high-use shopping timeframe between Thanksgiving and the end of the year, don't be bashful about checking your credit card statements every couple of days, and checking "recent transactions" to identify any fraudulent activity. If you find a charge which is not yours and appears fraudulent, don't waste time – report it via the card's online portal, mobile app, or by calling the card's customer service line. The quicker you report fraudulent activity, the faster you can protect yourself, and others, from additional fraudulent activity.

A list of 10 things you should be doing to protect yourself online can be daunting, but the bottom line is to shop wisely, make sure your own systems are protected, and to check your statements to identify potential fraud as soon as possible. Those three steps, and a little paranoia, can help make your holiday shopping experiences a little safer.

'Tis the Season…for Magecart!

Lead Analyst: Danika Blessman

We may have made it safely through Black Friday and Cyber Monday, but cybercrime is the gift that has the potential to "keep on giving" throughout the holiday shopping season. One such threat, a credit card-skimming collective dubbed Magecart, is suspected of having infiltrated over 100,000 ecommerce sites during the last year.

Magecart has become an umbrella term for at least seven cybercriminal groups using the same malware to achieve the same end by placing digital credit card skimmers on compromised ecommerce sites to harvest credit card data at an increasing rate with alarming success.

Researchers[1] differentiate the various groups based on unique infrastructure, skimmers, and targeting tactics. Although the goal is the same, tactics, techniques and procedures (TTPs) between the groups vary widely. Some groups cast a wide net, hoping to infect as many sites as possible. These likely use automated tools to breach sites and skim card data. Other groups are more selective in their targeting, possibly to secure a higher volume of transactions. Some groups are more advanced in their methods, hiding in plain sight and employing sophisticated methods to avoid detection. The groups do not appear to be affiliated with one another, but rather, are competitors in skimming credit card information for profit.

Researchers report[2] that there have been over 319,000 instances of Magecart during 2018, almost 90,000 of which were identified between August and October.

An increase in instances of Magecart seem to be reappearing just in time for what could be a record-breaking online shopping season.

Frighteningly, one-in-five online retailers which have remediated Magecart infections will be re-infected – sometimes within a week.

Shoppers in a panic to get all their holiday gifts in time might be more apt to click on links – or be unaware of using an unsecured (meaning, a site using HTTP instead of HTTPS) in their rush, increasing the chances of their credit card data being stolen.

Consumers can lessen their chances of the theft and misuse of their card data by following the ten tips in the previous article, *Protecting Yourself During the Holidays.*

And perhaps, most importantly, beware of deals that are just too good to be true.

Happy Holidays!

[1] https://www.bankinfosecurity.com/magecart-cybercrime-groups-harvest-payment-card-data-a-11700
[2] https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-2018-Black-Friday-E-Commerce-Blacklist.pdf

Apache Struts Vulnerabilities: Top on Attackers' Wish Lists

Lead Analyst: Terrance DeJesus

In November, GTIC researchers analyzed attackers targeting clients in the retail industry. GTIC researchers found that attackers were leveraging Apache Struts vulnerabilities in 58 percent of all attacks in the sector.

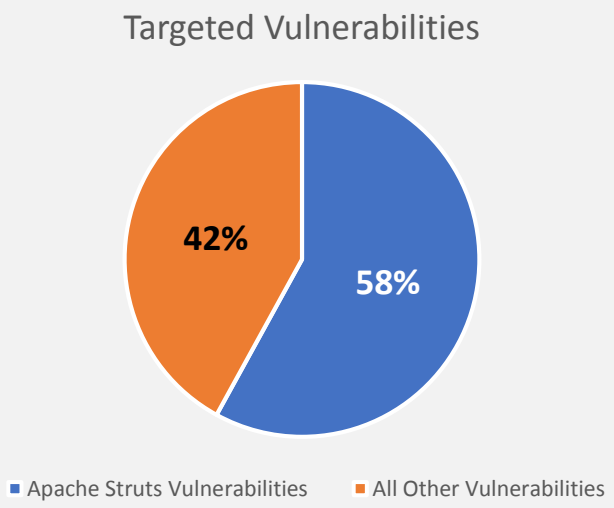
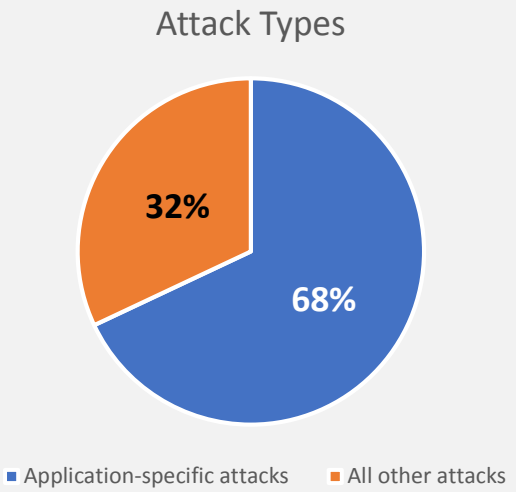


Figure 1. Targeted vulnerabilities in the retail industry

The Apache Struts-related attacks included older vulnerabilities, including CVE-2017-9791[3], CVE-2017-9805[4], CVE-2016-3087[5], and CVE-2017-5638[6].

[3] https://nvd.nist.gov/vuln/detail/CVE-2017-9791
[4] https://nvd.nist.gov/vuln/detail/CVE-2017-9805
[5] https://nvd.nist.gov/vuln/detail/CVE-2016-3087
[6] https://nvd.nist.gov/vuln/detail/CVE-2017-5638



Application-specific attacks accounted for 68 percent of all attacks within the retail sector during the month of November. Of these application-specific attacks, public facing servers with OpenSSL were targeted heavily, along with Apache Struts.

GTIC researchers found that attackers sought use-after-free (UAF) vulnerabilities which could allow remote code execution (RCE).

Figure 2. Attack types targeting the retail industry

Attackers targeted IoT devices with dictionary or brute-force attacks, specifically targeting routers and CCTV devices. Analysis indicates username and password credentials used by attackers were either extremely common, such as “admin:admin” or default login credentials for the targeted devices. In addition, GTIC researchers also observed exploit attempts against these routers and CCTV devices.

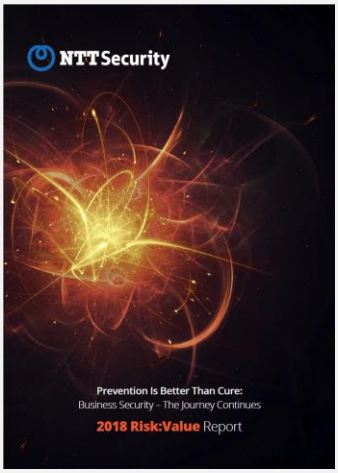
GTIC researchers’ analysis indicates these connection and exploit attempts are likely occurring via IoT botnets attempting to propagate. Once spread, attackers could use IoT botnets to launch an attack against other organizations.

NTT Security recommends the following:

For enterprises in the retail industry, ensure your networks, as well as your websites, are secure.

- Test and install the latest security patches for the systems in your network environment.
- Avoid using default or common username/password combinations for IoT device management.
- Implement a layered defensive strategy in your network environment to make it more difficult to would-be attackers to traverse your network.

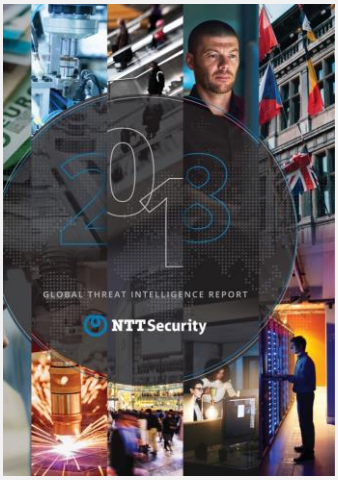
NTT Security Annual Reports



Risk:Value 2018

Many organizations are stuck in a reactive mindset when it comes to information security and would opt to pay a hacker's ransom rather than proactively invest in security. That's a key finding in this year's Risk:Value 2018 Report.

Download your copy today!



2018 Global Threat Intelligence Report

This year's report summarizes activity we detected in over 6.1 trillion+ logs and more than 150 million+ attacks, along with vulnerability scans, incident response engagements, and diverse findings from threat research and threat intelligence teams across NTT Security.

Download your copy today!

About GTIC

The NTT Security GTIC protects and informs NTT Group clients through security threat research, vulnerability analysis and the development of effective countermeasures. For more information, including vulnerability disclosures, threat reports and white papers, visit the resource page on www.nttsecurity.com or our blog.