NTT Security

GTIC Monthly Threat Report

March 2019

A Global Threat Intelligence Center
publication from NTT Security

Contents

The Dark Web: More Than Just a Clearinghouse for Your Personal Data

Lead Analyst: Danika Blessman

You may think your data being on the dark web is just a privacy concern, but it could have farther-reaching implications. It's not necessarily an individual concern, but it could also affect the threat to your entire organization's overall security.

The dark web is enabling attackers to successfully conduct attacks[1]. More specifically, the data acquired from breaches is being sold/traded on the dark web, and this activity is enabling attacks, due in no small part to the reuse of passwords.

From an individual's perspective, if you have any online accounts – banking, retail, airline rewards, social media, library card – it is almost guaranteed that at least some of that information has been compromised and is for sale or trade on the dark web. Furthermore, your risk is increased if you reuse passwords across multiple accounts. One attack method, known as credential stuffing, applies the same login credentials across multiple targeted sites. Quite often, these credentials work, causing further dissemination of data – or even a major breach, should one of these sets of credentials allow attackers access to individual systems or networks. Attackers can further exploit the network by moving laterally, elevating privileges, and accessing sensitive data for further exploitation.

The accumulation of all these details can put an individual at risk of an attack – quite often through phishing emails.

For example, an individual whose login information is compromised may be targeted by additional phishing or spear phishing attacks. If that individual is compromised and then connects to their employer's network, the phishing attack could potentially put the entire network at risk, as attackers often move laterally through a network after gaining access to one host or legitimate credentials. This is often the case in a BYOD scenario, or in the case where remote personnel can log in to company systems from outside the company network.

The dark web could also pose a threat to an organization from the perspective of an insider threat, as it can be used as a "dead drop" of sorts, or a neutral place for two parties who wish to anonymously exchange information – like individual or company data.

From a business perspective, this could be selling reused credentials, or could include insiders selling sensitive documents, amounting to corporate espionage. Access through non-conventional web browsers used to access the dark web may not be viewable in security logs, further hiding this activity. Some browsers are built to obscure all activity occurring within the browser, hiding potentially malicious activity.

[1] https://threatpost.com/dark-web-enterprise-security/142399/

What it boils down to is this: the more information attackers have about an organization – or an individual in an organization – the more effectively they can select – and successfully compromise – their targets.

There are innumerable ways stolen data on the dark web could be used to impact both individuals and organizations, but the above may prove to be the more immediate dangers. And these are real challenges organizations face on a daily basis, but there are some simple things you can do to help prevent this type of activity.

If you haven't changed your password since login credentials were affected in one of what feels like never-ending string of breaches, it's time to do so. Also, ensure you are not reusing passwords across multiple sites, which greatly increases the probably of success for credential stuffing attacks. Using strong, unique passwords and enabling multi-factor authentication are two of the easiest things a user can do for the sake of security.

In addition, consider segmenting your network and enforcing "least privilege," so even those with legitimate credentials can only access certain areas of the network. And a good network monitoring solution can help in detecting anomalous activity, such as normal users logging in at odd times or sensitive data being exfiltrated from your network.

Educate users and analyze your organization's security posture. Enforce strong, unique passwords for users in your organization, segregate networks, and leverage a defense-in-depth strategy to enhance your company's cyber resilience.

Patch This Zero-Day Vulnerability!

Lead Analyst: Aaron Perkins

If you or your organization are like many others, you use Google Chrome as your preferred internet browser.

In fact, according to Statcounter[2], over 57 percent of internet browsing occurs in the Google Chrome browser, with Apple's Safari browser coming in at a distant second with less than 15 percent market share.

With this high of an amount of internet browsing taking place via Google Chrome, it comes as no surprise that a recent zero-day vulnerability in the browser prompted Google to react quickly and roll out patches across the globe.

If successfully exploited, this zero-day vulnerability (CVE-2019-5786) would allow an attacker to execute arbitrary code in the context of the browser[3].

This vulnerability allows an attacker to execute arbitrary code in the context of the browser.

Worse yet, security researchers have discovered evidence that this vulnerability has been widely exploited in the wild. And, systems not yet patched for this vulnerability allow attackers to continue to leverage this exploit.

Google has been relatively quiet though on the details of the vulnerability, citing a need to implement the security patch across as many devices as possible before revealing further details.

At any given point, Google has multiple versions of Google Chrome available on a variety of platforms. For the enterprise environment on Windows, Mac, and Linux machines, the version your organization should be implementing is the **stable channel** version of Google Chrome.

As of this writing, the updated version of the software is 73.0.3683.86 for Windows, Mac, and Linux, which, according to the Chrome Releases blog[4], will roll out over the coming days and weeks.

NTT Security recommends testing and implementing the latest stable version of the software as early as possible to mitigate risks associated with this zero-day vulnerability.

For more information on how to update Google Chrome, visit the official Google Chrome Help Site.

[2] http://gs.statcounter.com/
[3] https://www.cisecurity.org/advisory/a-vulnerability-in-google-chrome-could-allow-for-arbitrary-code-execution_2019-026/
[4] https://chromereleases.googleblog.com/

4G and 5G Networks Could Let Hackers Track Your Location

Lead Analyst: Danika Blessman

Researchers[5] from Purdue University and the University of Iowa have uncovered yet another set of vulnerabilities in the way our wireless devices communicate – this time affecting the paging protocols used to notify devices about incoming communications.

According to the research team, this could, in turn, allow attackers to intercept calls, send fake notifications or alerts, and even track users' locations, alerts, or other notifications, breaking privacy in both the 4G and 5G mobile protocols.

The basis of these vulnerabilities lies in the way mobile devices conserve battery life by only polling for pending services periodically. The researchers go on to explain, "When there is a phone call or an SMS message for the device, it needs to be notified. This is achieved by the paging protocol, which strives to achieve the right balance between the device's energy consumption and timely delivery of services such as phone calls."

This could allow attackers to intercept calls, breaking privacy in both the 4G and 5G mobile protocols.

Researchers discovered three separate attack methods based on that paging mechanism. The primary attack has been dubbed "ToRPEDO," short for Tracking via Paging Message Distribution, and can be used to verify the location of a given device, allowing attackers to potentially send fake notifications or perform a denial of service on the device.

ToRPEDO leverages all available data, including the exact time delay between when the call is made and when the user is notified of the incoming call, and the exact number of paging records for each instance.

ToRPEDO also enables two other attack methods. The first of these two methods is PIERCER, short for Persistent Information Exposure by the Core Network, which has the capability to determine an International Mobile Subscriber Identity (IMSI) – essentially a device's unique ID number. The second method is the aptly-named IMSI-cracking attack which can brute force an IMSI number in both 4G and 5G networks, where IMSI numbers are encrypted.

Per the researchers, all four major U.S. cellular providers are affected by ToRPEDO, and attacks can be carried out with equipment costing as little as a couple hundred dollars. At least one U.S. mobile network is also susceptible to the PIERCER attack. Because these attacks affect 4G and 5G, almost all cellular networks outside the U.S. are vulnerable as well, including several providers in Europe and Asia.

Given the nature of these attacks, the researchers have opted not to release the proof-of-concept code.

[5] https://www.documentcloud.org/documents/5749002-4G-5G-paper-at-NDSS-2019.html

As NTT Security analysts described in a blog[6], although 5G promises enhanced security and privacy, it may not be able to fully deliver, as it inherits flaws in security and protocols from previous generations.

This warning from researchers to manufacturers and providers is not new. In March 2018, many of the same researchers revealed[7] flaws in the LTE protocols. Since 5G is using the same protocols as 4G, the flaws will remain, impacting the entire industry and, by extension, many mobile device users.

Frustratingly, users are not able to protect themselves from these vulnerabilities. The onus is on telecom providers to protect their end users. Continued research and revelation of these vulnerabilities will hopefully apply enough pressure to get these flaws resolved.

[6] https://technical.nttsecurity.com/post/102fdn9/5g-a-blessing-or-a-curse-to-iot
[7] https://www.theregister.co.uk/2018/03/05/4g_lte_protocol_vulnerabilities/

Briefly Analyzing Web Browser Statistics: MSS Data, Market Share, and Existing Vulnerabilities

Lead Analyst: Terrance DeJesus

Market-Share

In the wake of Google releasing a patch for the recent Stable Channel zero-day CVE-2019-5786, researchers from the NTT Security GTIC explored, from a statistical standpoint, the web browser threat landscape. Google's release[8] indicates Google was aware of reports that this vulnerability was being actively exploited in the wild. For more information on this vulnerability, check out the article, Patch This Zero-Day Vulnerability, in this publication.

Since May 2009, as shown in Figure 1, Google Chrome use has been on the rise, while popular web browsers, installed by default, such as Internet Explorer, have rapidly declined. Considering Google Chrome was released in 2008, it is likely that most Windows users were still using Windows Vista. Of the many benefits Google Chrome has over Internet Explorer, many found interest in its speed, thanks to its V8 JavaScript engine. Internet Explorer was built using Trident but could not compete with the speed of Chrome's engine. Rife with vulnerabilities, Trident was thrown to the side in 2014 to create EdgeHTML for Microsoft Edge on Windows 10. At the time of this writing, Chrome held roughly 57 percent of the web browser market share where 8 out of 10 of the top platforms are either Windows or Android based.

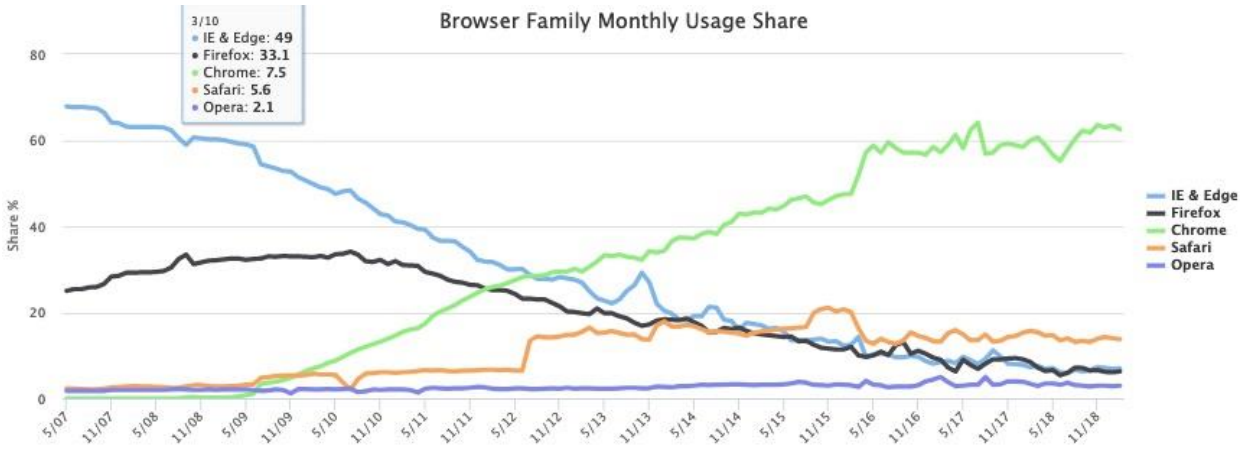


Figure 1. Browser family monthly usage share[9]

[8] https://chromereleases.googleblog.com/2019/03/stable-channel-update-for-desktop.html
[9] https://www.w3counter.com/globalstats.php

Web Browser Vulnerabilities in Existence

Researchers reviewed the number of web browser vulnerabilities over the years, additionally answering other questions, to include identifying those vulnerabilities which allowed remote code execution (RCE). Figure 2 shows volumes of web browser vulnerabilities for the most popular web browsers over time as well as which of these vulnerabilities, if successfully exploited, allowed RCE. Figure 3 shows those which did not allow RCE. As shown, vulnerabilities within web browsers typically allow RCE if successfully exploited. Until roughly 2015, there was a sharp increase in vulnerabilities found for Mozilla Firefox, Google Chrome, and Microsoft Edge, though these do not typically allow RCE.

It may seem odd that a majority of vulnerabilities in web browsers allow RCE. Typically, these browsers contain many subsystems for functionality such as HTML rendering, JavaScript engines, CSS parsers, image parsers, etc. The smallest coding error could result in a vulnerability, which, if exploited, could allow arbitrary code execution. Over the years, companies like Mozilla, Microsoft, and Google have focused more on the inner-workings of browser security. This could possibly explain why more vulnerabilities are found, but those which are found are usually not as great a threat. A downside to this security is as web browsers become more secure, attackers seek to compromise popular websites to infect victims, often manipulating Document Object Models (DOM) in the source code. If properly exploited, the website renders normally, without the victim realizing anything is amiss. DOM objects often link to JavaScript code on the page, and, if manipulated, could easily allow the attacker to take additional actions, like sending a download request to a remote server for malware.

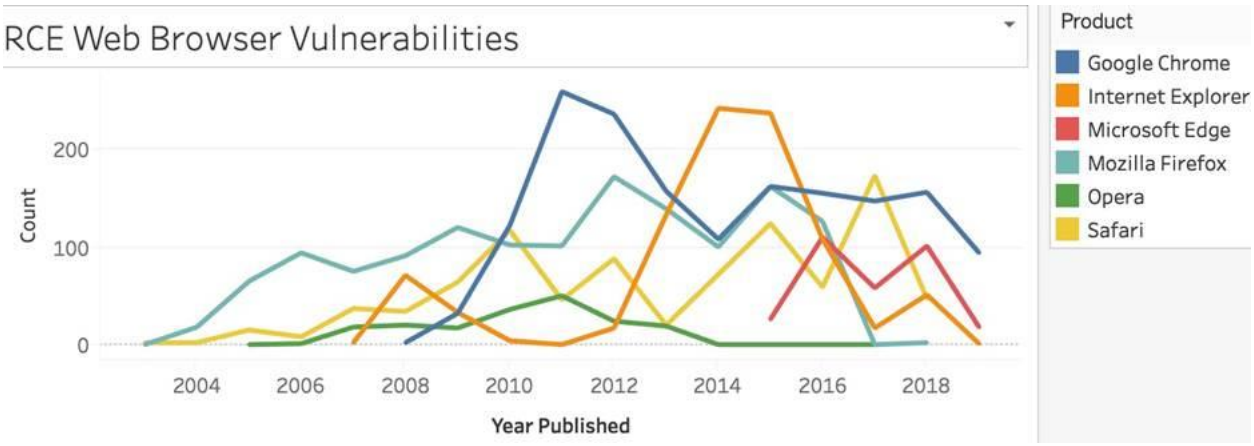


Figure 2. Web browser vulnerabilities over time with remote code execution

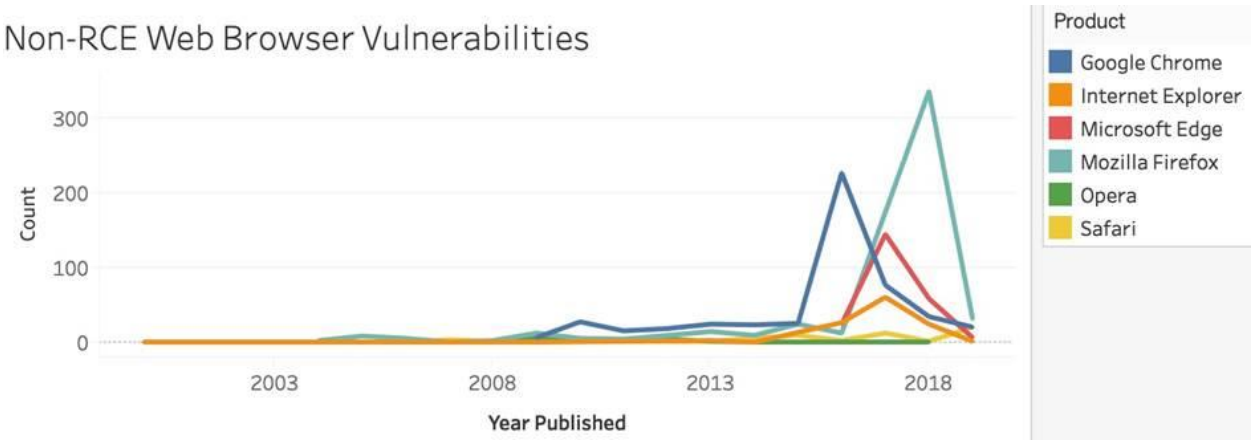


Figure 3. Web browser vulnerabilities over time without remote code execution

Exploits found in third-party plugins for specific web browsers have become threat actors' chosen vector for drive-by downloads. Examples are Adobe Flash Player, notorious for RCE vulnerabilities, as well as Microsoft Silverlight, and Java, all heavily targeted in malware campaigns. In addition, web browsers are the primary interface between a user and the internet, creating a target-rich environment for all threat actors – from script kiddies to Advanced Persistent Threat (APT) groups.

MSS Data Observations for Web Browser Attacks

According to MSS data from 2018, only Chrome, Edge, Internet Explorer, and Firefox attacks were observed as targeted web browsers. In fact, 84 percent of all attacks against web browsers in 2018 focused on Internet Explorer. Figure 4 shows that attacks against IE declined from November 2017 through July 2018, where Edge attacks started to increase and had similar volume. One theory attributing to this activity is the continuing adoption of Windows 10 and Edge in corporate environments, prompting threat actors to upgrade their arsenals and increase focus on Edge.

It is surprising to see relatively few attacks against Chrome, though, considering it has greater than a 60 percent market share, as shown in Figure 1. When comparing Figures 1 and 4, as the market share for Internet Explorer plummets, so do the number of attacks against it; however, we do not observe the same pattern in the increase of Google Chrome usage and then attacks.

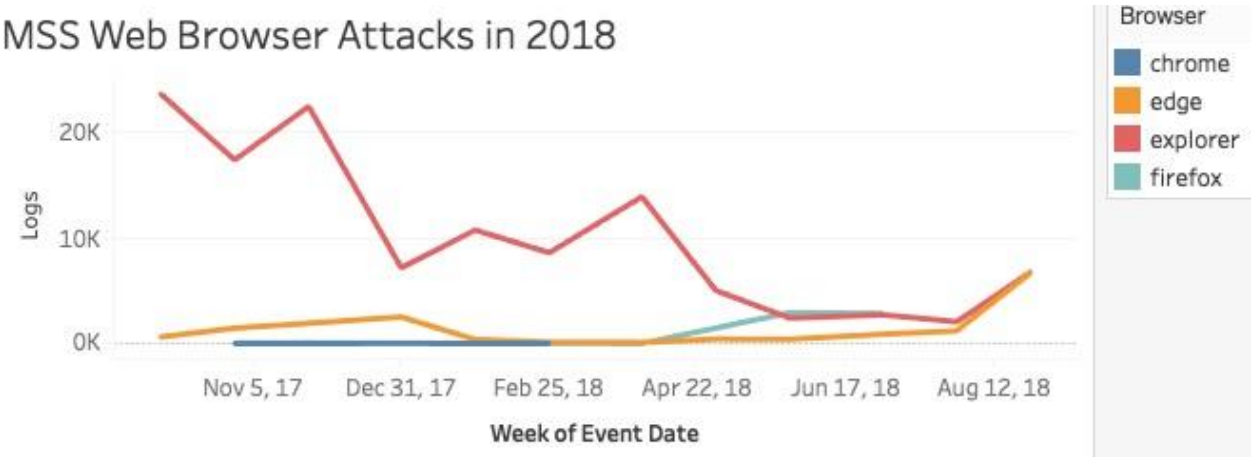


Figure 4. Web browser attacks from MSS data

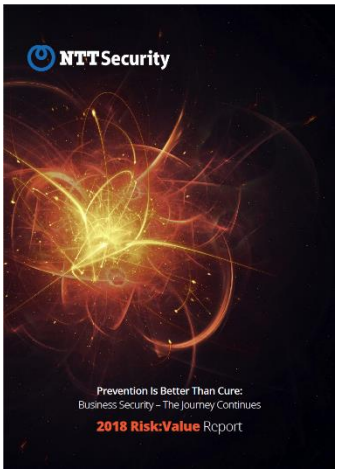
When reviewing web browser attacks against Internet Explorer, most attacks primarily target a memory corruption vulnerability, Adobe Flash Player library issue, or DLL side-loading exploit[10]. Memory exploits appear to be common where attackers attempt to take advantage of use-after-free (UAF) vulnerabilities[11].

Final Thoughts

From the data GTIC security researchers analyzed, the browser with the greatest market share is Google Chrome, although attacks against Google Chrome are far less common than those against either Internet Explorer or Edge. A higher market share often helps determine the likeliness of which products hackers may choose to focus on, especially if it increases chances of infection. Regardless of web browser, though, organizations should ensure application whitelisting includes which browsers are acceptable, along with maintaining proper patch management for this software. Additional layered-defense tactics will help mitigate web browser attacks. Chromium-based browsers such as Chrome contain mitigation techniques such as site isolation[12] and multi-process architecture[13] which will help guard against web browser attacks.

[10] https://attack.mitre.org/techniques/T1073/
[11] https://www.purehacking.com/blog/lloyd-simon/an-introduction-to-use-after-free-vulnerabilities
[12] https://www.chromium.org/Home/chromium-security/site-isolation
[13] https://www.chromium.org/developers/design-documents/multi-process-architecture

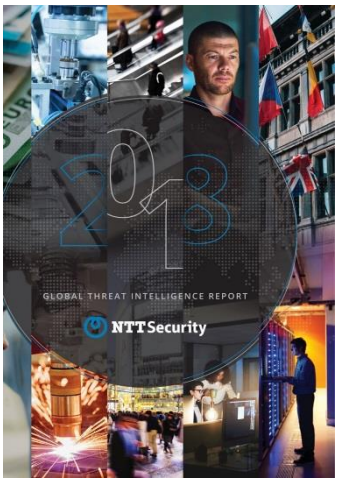
NTT Security Annual Reports



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.

About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit nttsecurity.com to learn more about NTT Security or visit www.ntt.co.jp/index_e.html to learn more about NTT Group.